Panel de Mobile Security de Junos Pulse

Guía de administración

Versión
3.0

Noviembre de 2011
R2

Copyright © 2011, Juniper Networks, Inc.

.

Panel de Mobile Security de Junos® Pulse

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
408-745-2000
www.juniper.net

Copyright © Juniper Networks, Inc.
Noviembre de 2011

Juniper Networks, Junos, Steel-Belted Radius, NetScreen y ScreenOS son marcas comerciales registradas de Juniper Networks, Inc. en los Estados Unidos y otros países. El logotipo de Juniper, el logotipo de Junos y JunosE son marcas registradas de Juniper Networks, Inc. Todas las demás marcas comerciales, marcas de servicio, marcas comerciales registradas o marcas de servicio registradas pertenecen a sus respectivos propietarios. Juniper Networks no asume responsabilidad alguna por ningún error en el contenido del presente documento. Juniper Networks se reserva el derecho de cambiar, modificar, transferir o, de cualquier otra manera, modificar esta publicación sin previo aviso. Los productos fabricados o comercializados por Juniper Networks o sus componentes podrían estar incluidos en una o más de las siguientes patentes que posee en propiedad o mediante licencia a Juniper Networks: patentes de EE.UU. n.º 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186 y 6,590,785. Derechos de autor © 2011, Juniper Networks, Inc. Todos los derechos reservados.

Índice

Público v
Contenido de la guía v
Convenciones tipográficas v
Comuníquese con soporte técnico vi
Capítulo 1 **Introducción** 1
Funciones del panel de Mobile Security de Junos Pulse 1
Capítulo 2 **Adición de dispositivos al panel de Mobile Security de Junos Pulse (para los proveedores de servicio)** 1
Configuración del panel de Mobile Security de Junos Pulse para los consumidores 1
Capítulo 3 **Instalación y registro de Junos Pulse en dispositivos móviles** 3
Información general sobre la instalación - Todas las plataformas 3
Instrucciones de instalación y registro para Android 3
Registro de seguridad 4
Registro automático mediante URL 4
Registro manual 5
Instrucciones de instalación y registro para BlackBerry 9
Registro de seguridad 9
Registro automático 9
Registro manual 10
Funciones disponibles de Junos Pulse 10
Instrucciones de instalación y registro para iOS 11
Instrucciones de instalación y registro para Windows Mobile 16
Capítulo 4 **Utilización del panel de Mobile Security** 21
Información general 21
Comandos y eventos de la ficha Inicio 22
Comandos 22
Comandos para los dispositivos iOS 23
Eventos 24
Eventos para dispositivos iOS 25
Información y configuración de la ficha Ajustes 26
Administración de cuentas 26
Administración del teléfono 26
Información y configuración de la ficha Reportes 29
Historial 30
Información y configuración de la ficha Configuración de alerta 30
Información y configuración de la ficha Soporte/Ayuda 32

Capítulo 5 **Utilización de Junos Pulse en los dispositivos móviles** 33
Funciones de seguridad en Android 33
Estado 34
Adición de una conexión segura 35
Conexión 36
Visualización del estado de la conexión 36
Visualización de la pantalla de estado de la conexión 37
Utilización de las funciones de seguridad 38
Registro de seguridad 38
Registro automático mediante URL 38
Registro manual 39
Antivirus 40
Detección de malware, aplicaciones prohibidas y aplicaciones sospechosas 42
Pantalla de resultados del análisis 42
Fichas con los resultados del análisis 42
Supervisión y control 47
Respaldo de datos 47
Ajustes de seguridad 48
Funciones antirrobo 49
Desinstalación o borrado de datos 50
Funciones de seguridad de BlackBerry 51
Antivirus 51
Análisis de virus manual 52
Archivos en cuarentena 53
Análisis a demanda 54
Registro de supervisión de archivos 54
Supervisión y control: 54
Respaldo & Restaurar 54
Ajustes 55
Funciones antirrobo 55
Funciones de seguridad iOS 56
Conexión con Junos Pulse 57
Adición de un perfil de conexión segura 58
Conexión 60
Visualización del estado de la conexión 60
Funciones de seguridad de Windows Mobile 61
Estado 61
Conexión 61
Conectar 61
Correo electrónico e Intranet 61
Utilización de las funciones de seguridad 62
Ajustes de seguridad 63
Antivirus 63
Antispam 64
Cortafuegos 66
Supervisión y control 69
Respaldo de datos 69
Funciones antirrobo 70
Capítulo 6 **Preguntas frecuentes de Junos Pulse** 73
Preguntas frecuentes de Junos Pulse 73

Copyright © 2011, Juniper Networks, Inc.

Acerca de esta guía

Esta guía describe cómo crear directivas de seguridad utilizando el panel de Junos® Pulse Mobile Security y cómo instalar y utilizar el software de Junos Pulse en los dispositivos admitidos.

Público

Esta guía se ha creado para los usuarios que deseen configurar controles para los usuarios de dispositivos, ofreciendo funciones de seguridad y de control de acceso.

Contenido de la guía

Esta guía tiene los capítulos siguientes:

- Capítulo 1, “Introducción” en la página 1
- Capítulo 2, “Instalación y registro de Junos Pulse en dispositivos móviles” en la página 3
- Capítulo 3, “Utilización del panel de Mobile Security” en la página 21
- Capítulo 4, “Utilización de Junos Pulse en los dispositivos móviles” en la página 33

Convenciones tipográficas

La Tabla 1 describe las convenciones de texto utilizadas en la guía.

Tabla 1: Convenciones tipográficas

Convención	Descripción	Ejemplos
Negrita	Indica botones, nombres de campos, nombres de diálogos y otros elementos de la interfaz de usuario.	Utilice las fichas Programación y Citas para programar una reunión.
Letra de palo seco sencilla	Representa: • URL, nombres de archivos y directorios	Ejemplo: • URL: Descargue la aplicación JRE en: http://java.sun.com/j2se/
Cursiva	Identifica: • Términos definidos en el texto • Elementos variables • Títulos de libros	Ejemplos: • Elemento variable: Utilice los ajustes de la página UUsers Usuarios) > Roles (Funciones) > Select Role page to configure roles (Seleccionar función para configurar las funciones).

Copyright © 2011, Juniper Networks, Inc.

Comuníquese con soporte técnico.

En el Centro de asistencia técnica de Juniper Networks (JTAC) podrá obtener soporte técnico para los productos. Si usted es un cliente con un contrato de asistencia de J-Care o JNASC activo o está cubierto por la garantía y necesita asistencia técnica postventa, puede obtener acceso a nuestras herramientas y recursos en línea o abrir un caso con JTAC.

- Directivas de JTAC: para conocer todas nuestras directivas y procedimientos de JTAC, revise la Guía del usuario de JTAC en http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Garantías del producto: para obtener información sobre la garantía del producto, visite http://www.juniper.net/support/warranty/.
- Horas de operación de JTAC: Los centros de JTAC tienen recursos disponibles 24 horas al día, 7 días a la semana, 365 días al año.

Copyright © 2011, Juniper Networks, Inc.

Capítulo 1

Introducción

El panel de Junos® Pulse Mobile Security recopila datos de dispositivos móviles designados y carga estos datos a un panel al que se puede acceder a través de Internet con un nombre de usuario y contraseña. Al utilizar el panel de Mobile Security de Junos Pulse, podrá administrar los dispositivos móviles registrados y habilitar funciones como la limpieza remota en caso de pérdida o robo de un dispositivo. También podrá configurar alertas de correo electrónico en caso de que el dispositivo móvil se utilice para enviar o recibir mensajes sospechosos. En este caso, los mensajes que contengan palabras clave personalizadas, como drogas o alcohol, o los mensajes que provengan de direcciones específicas o vayan destinados a ellas, se le enviarán por correo electrónico de forma automática.

Funciones del panel de Mobile Security de Junos Pulse

El panel de Mobile Security de Junos Pulse ofrece control y seguridad para los dispositivos móviles registrados.

Entre las funciones de control se incluyen:

- Supervisión de la actividad en el dispositivo.
- Visualización de imágenes tomadas con la cámara del dispositivo y enviadas o recibidas por texto o correo electrónico.
- Visualización del contenido de todos los mensajes de texto y de correo electrónico.
- Recepción automática de alertas cuando se encuentran palabras clave en los mensajes recibidos o enviados.
- Lista de todas las aplicaciones y software instalados en el dispositivo.
- Visualización de la ubicación del dispositivo en un mapa en línea.
- Sonido y alarma en el dispositivo.
- Utilización de GPS para localizar el dispositivo en caso de pérdida o robo. (la función de GPS puede no estar disponible en los teléfonos inteligentes Verizon BlackBerry Curve o Storm 1). Si recibe unas coordenadas de longitud y latitud 0.0 del GPS, es posible que el proveedor del servicio haya bloqueado esta función o que el dispositivo no reciba la señal del satélite).

Copyright © 2011, Juniper Networks, Inc.

Entre las funciones de seguridad se incluyen:

- Antivirus: esta función ofrece una protección en tiempo real frente a amenazas de malware gracias al análisis automático de los dispositivos para garantizar que los archivos no están infectados con malware. La función de análisis cuando la solicite le permite analizar archivos y carpetas seleccionados para garantizar que el dispositivo y la tarjeta de memoria están limpios y protegidos. La función de actualización automática garantiza que el dispositivo cuente con las últimas firmas de antivirus.
- Respaldo & Restaurar: esta función le permite respaldar los contactos y la información del calendario.
- Cortafuegos: las funciones de seguridad del cortafuegos le permiten bloquear o permitir el tráfico de datos hacia o desde el dispositivo usando listas de reglas que controlan el tráfico en base al número de puerto y dirección IP.
- Antirrobo: este conjunto de funciones incluye comandos remotos que puede enviar al dispositivo en caso de pérdida o robo. Estos comandos incluyen el bloqueo del dispositivo, limpieza del dispositivo, ubicación del dispositivo y respaldo del dispositivo.

Copyright © 2011, Juniper Networks, Inc.

Capítulo 2

Adición de dispositivos al panel de Mobile Security de Junos Pulse (para los proveedores de servicio)

Antes de que los consumidores puedan utilizar Junos® Pulse, deberá realizar algunas tareas preliminares para preparar el panel Junos Pulse Mobile Security y dejarlo listo para su uso.

Configuración del panel de Mobile Security de Junos Pulse para los consumidores

Realice las tareas siguientes para que el consumidor pueda acceder al panel y utilizar las funciones disponibles.

1. Inicie sesión en el panel de Mobile Security de Junos Pulse utilizando la dirección URL siguiente en el navegador e ingresando las credenciales que se le han proporcionado.

   https://mss.junospulse.juniper.net

2. Una vez que haya iniciado sesión, seleccione la ficha **Devices** (Dispositivos).
3. Haga clic en **Add** (Agregar) para abrir el cuadro de diálogo **Add Device** (Agregar Dispositivo).
4. Especifique lo siguiente:
   - **Número de teléfono:** introduzca el número de teléfono del dispositivo, incluido el código de país y el código de área. Por ejemplo, 16035551212.
5. Haga clic en **Save** (Guardar). La puerta de enlace utiliza SMS para enviar al dispositivo un enlace de descarga del software Junos Pulse y una clave de licencia para el consumidor.

Nota informativa: los proveedores de servicios pueden crear una API que anule estas instrucciones de distribución. Si es así, consulte la información del proveedor de servicios.

Cuando el usuario hace clic en la URL proporcionada y específica de la plataforma del dispositivo, se descargará Junos Pulse. Deberá entonces proporcionar la clave de licencia para registrar el producto y crear un nombre de usuario y contraseña durante el registro para iniciar sesión en el panel de Mobile Security.

Consulte la Guía de administración de Mobile Security Gateway de Junos Pulse para obtener más información.

Copyright © 2011, Juniper Networks, Inc.

 Copyright © 2011, Juniper Networks, Inc.

Capítulo 3

Instalación y registro de Junos Pulse en dispositivos móviles

Este capítulo describe el proceso de instalación y registro de Junos Pulse para cada plataforma admitida.

Información general sobre la instalación - Todas las plataformas

Como parte del proceso de instalación y registro, deberá realizar los pasos siguientes para todas las plataformas móviles admitidas:

- Descargue el software de Junos Pulse Security en el dispositivo móvil.
- Registre la aplicación Junos Pulse con el fin de utilizar las funciones del panel de Mobile Security basadas en la Web para configurar e implementar las funciones de supervisión, control y seguridad.
- Cree un nombre de usuario y contraseña en el dispositivo como parte del proceso de instalación de Junos Pulse. Utilizará este nombre de usuario (el nombre de usuario y la dirección de correo electrónico) y la contraseña para iniciar sesión en el panel de Mobile Security en Internet. El nombre de usuario y la contraseña le permiten controlar y supervisar el dispositivo de forma efectiva, por lo que no deberá proporcionar esta información al usuario del dispositivo. Asimismo, las alertas de correo electrónico se envían a la dirección de correo electrónico proporcionada como nombre de usuario. Por lo tanto, esta dirección de correo electrónico no debe ser la del usuario del dispositivo.

Instrucciones de instalación y registro para Android

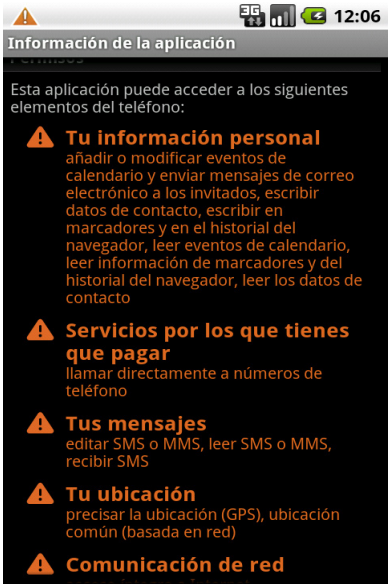
Utilice las instrucciones siguientes para descargar e instalar el software de Junos Pulse en los dispositivos con Google Android.

Nota informativa: el cliente Junos Pulse está disponible en la tienda de aplicaciones de Android.

1. Desde el dispositivo con Android, descargue el software de Junos Pulse directamente al dispositivo. Una vez descargado, Junos Pulse se instala automáticamente.
2. Durante la instalación, se le solicitará que permita a la aplicación utilizar los componentes de llamadas telefónicas y de comunicación de red. Seleccione **OK** (Aceptar). Consulte la Figura 1 en la página 4.

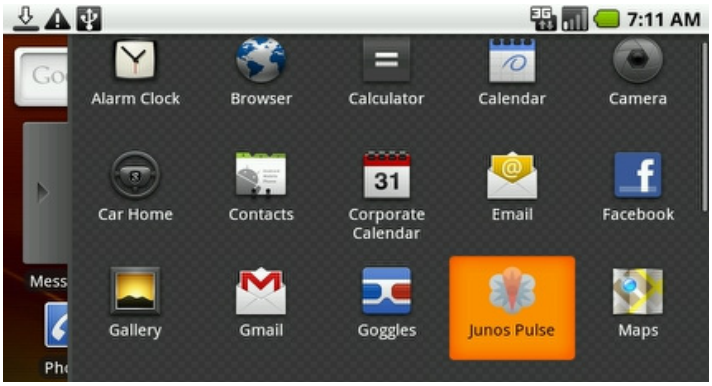
Copyright © 2011, Juniper Networks, Inc.

Figura 1: Permita que Pulse utilice las comunicaciones de red


12:06
Información de la aplicación
Esta aplicación puede acceder a los siguientes elementos del teléfono:
Tu información personal
añadir o modificar eventos de calendario y enviar mensajes de correo electrónico a los invitados, escribir datos de contacto, escribir en marcadores y en el historial del navegador, leer eventos de calendario, leer información de marcadores y del historial del navegador, leer los datos de contacto
Servicios por los que tienes que pagar
llamar directamente a números de teléfono
Tus mensajes
editar SMS o MMS, leer SMS o MMS, recibir SMS
Tu ubicación
precisar la ubicación (GPS), ubicación común (basada en red)
Comunicación de red

Una vez que la aplicación se ha descargado e instalado, el icono de Junos Pulse aparecerá en el menú de aplicaciones. Consulte la Figura 2 en la página 4.

Figura 2: Junos Pulse en el menú de aplicaciones



La primera vez que inicie Junos Pulse, se mostrará el Acuerdo de Licencia de usuario final. Debe **aceptar** la licencia para comenzar a usar Junos Pulse.

Registro de seguridad

Su administrador puede configurar el registro de seguridad en el dispositivo para que se realice de forma automática, mediante URL o de forma manual.

Registro automático mediante URL

Para realizar el registro automático mediante URL, tendrá que seleccionar una URL proporcionada por su administrador. Cuando haga clic en la URL, se le mostrará un mensaje para que verifique que dicha URL proviene de una fuente confiable. Al hacer clic en **Yes** (Sí) tras recibir este mensaje, tendrá lugar el proceso de registro de seguridad automático.

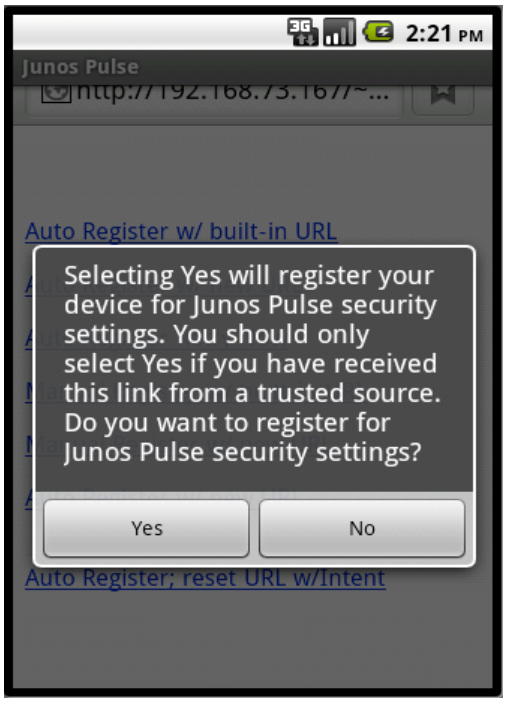
Copyright © 2011, Juniper Networks, Inc.

Para registrar las funciones de seguridad de forma automática, haga lo siguiente:

1. Inicie Junos Pulse.
2. Seleccione la URL de registro que le ha proporcionado su administrador por correo electrónico, mensaje de texto o sitio Web.
3. Debido a que el registro automático modifica los ajustes de seguridad de su dispositivo, deberá verificar la validez de la URL. Si está seguro de que la URL es confiable, seleccione **Yes** (Sí) cuando se le solicite (consulte la Figura 3 en la página 5).

Después de haber seleccionado Yes (Sí), el dispositivo estará registrado automáticamente para las funciones de seguridad.

Figura 3: Solicitud de registro automático mediante URL


2:21 PM
Junos Pulse
Auto Register w/ built-in URL
Selecting Yes will register your device for Junos Pulse security settings. You should only select Yes if you have received this link from a trusted source. Do you want to register for Junos Pulse security settings?
Yes
No
Auto Register; reset URL w/Intent

Registro manual

En algunos casos, el registro manual puede también solicitarle que seleccione una URL proporcionada por su administrador. Cuando seleccione la URL, se le mostrará un mensaje para que verifique que dicha URL proviene de una fuente confiable (consulte la Figura 4 en la página 6). Al hacer clic en Yes (Sí) en la solicitud de registro, se mostrará la pantalla de registro manual.

La pantalla de registro requiere que ingrese cierta información, como el código de licencia proporcionado por su administrador.

Nota informativa: si utiliza un dispositivo con WIFI solamente (como una tableta sin servicio celular), el campo del número de teléfono no se mostrará en la ventana de registro. Consulte la Figura 5 en la página 7.

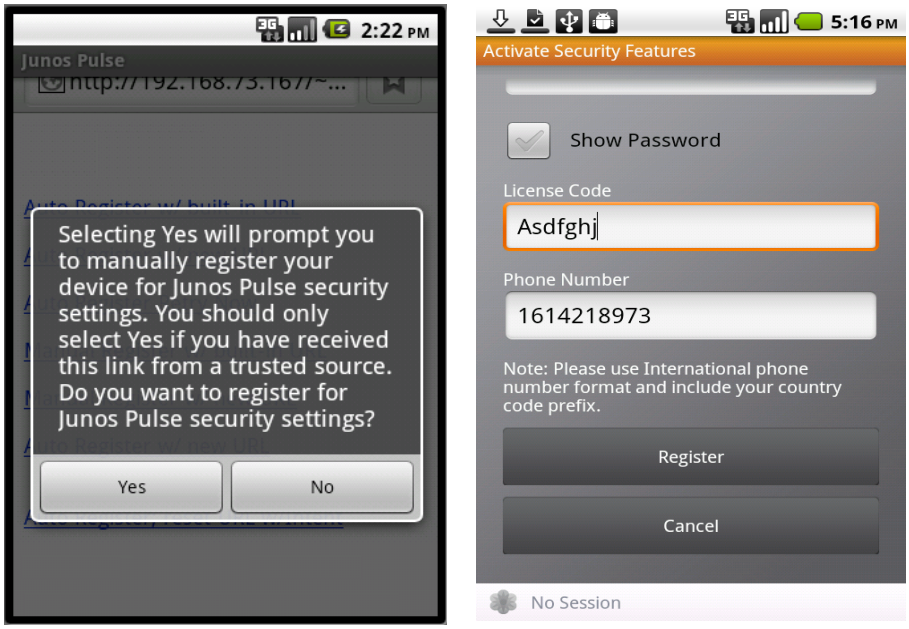
Copyright © 2011, Juniper Networks, Inc.

Para registrar manualmente la seguridad, realice lo siguiente:

1. Inicie Junos Pulse.

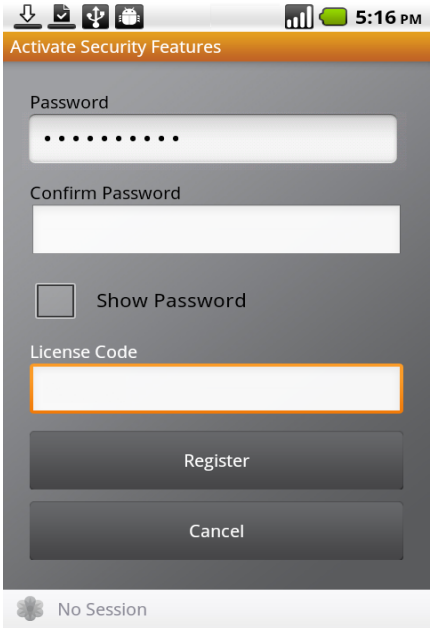
1. Seleccione la **URL** que le ha proporcionado su administrador por correo electrónico, mensaje de texto o sitio Web.
2. Compruebe que la URL es confiable y haga clic en **Yes** (Sí) cuando se le solicite. Aparecerá la pantalla de registro (consulte la Figura 4 en la página 6).
3. Opcionalmente, ingrese una dirección de Correo electrónico y Contraseña. (La información de correo electrónico y de contraseña no se usa en este momento.)
4. Especifique el **código de licencia** que le proporcionó su administrador.
5. El número de teléfono del dispositivo aparece en el cuadro **Número de teléfono**. Si el número no aparece, ingréselo manualmente, incluidos el código de país y el código de área sin los prefijos internacionales '00' ni '+'. No utilice espacios, paréntesis ni caracteres especiales.
6. Seleccione **Register** (Registrar).

Figura 4: Solicitud de registro manual mediante URL y pantalla de registro


2:22 PM
Junos Pulse
Selecting Yes will prompt you to manually register your device for Junos Pulse security settings. You should only select Yes if you have received this link from a trusted source. Do you want to register for Junos Pulse security settings?
Yes
No
5:16 PM
Activate Security Features
Show Password
License Code
Asdfghj
Phone Number
1614218973
Note: Please use International phone number format and include your country code prefix.
Register
Cancel
No Session

Copyright © 2011, Juniper Networks, Inc.

Figura 5: Ejemplo de registro manual para dispositivo con WIFI solamente



Una vez que haya registrado las funciones de seguridad correctamente, se mostrarán las funciones disponibles (consulte la Figura 6 en la página 8), a las que podrá acceder con el botón de seguridad (consulte la Figura 7 en la página 8). Estas funciones son las siguientes:

- **AntiVirus and Malware Detection** (Antivirus y detección de malware): control de las actividades del antivirus y detección de malware instalado.
- **Monitor and Control** (Supervisión y control): visualización de los ajustes de supervisión.
- **Backup Data** (Respaldar datos): respaldo de la información del calendario y los contactos.
- **Security Settings** (Ajustes de seguridad): ajuste los intervalos de los análisis de sistema.

El administrador puede habilitar o deshabilitar las funciones de seguridad.

Copyright © 2011, Juniper Networks, Inc.

Figura 6: Funciones disponibles

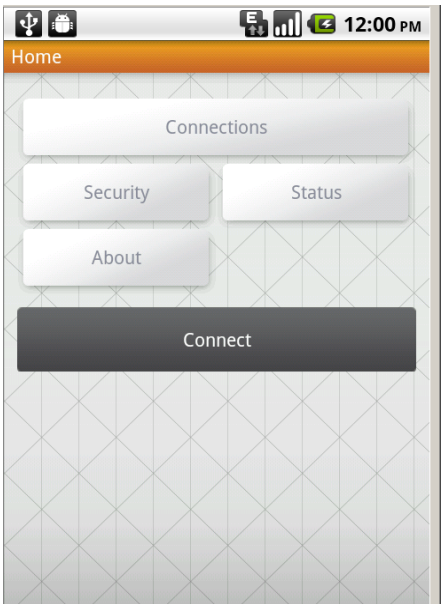
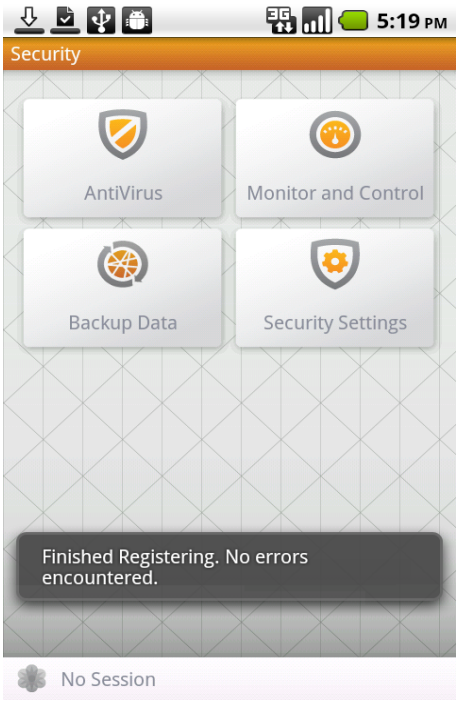


Figura 7: Funciones de seguridad



Consulte “Funciones de seguridad en Android” en la página 33 para obtener información sobre las funciones y la configuración de Junos Pulse en dispositivos con Android.

 Copyright © 2011, Juniper Networks, Inc.

Instrucciones de instalación y registro para BlackBerry

Utilice las instrucciones siguientes para descargar, instalar y registrar el software de Junos Pulse.

Nota informativa: Asegúrese de que los servicios de datos estén habilitados en el dispositivo de modo que pueda recibir actualizaciones de definiciones de virus y ajustes.

1. Por medio del navegador Web del dispositivo BlackBerry, descargue el software de Junos Pulse directamente en el dispositivo.
2. Abra la aplicación Junos Pulse desde el directorio **Application** (Aplicación) o **Download** (Descarga).
3. Deberá aceptar el acuerdo de usuario para poder comenzar la instalación. Utilice el botón **Menú** para acceder al menú que le permite aceptar el acuerdo. Después de seleccionar **I agree** (Acepto), comenzará la instalación y el registro. Consulte la Figura 8 en la página 9.

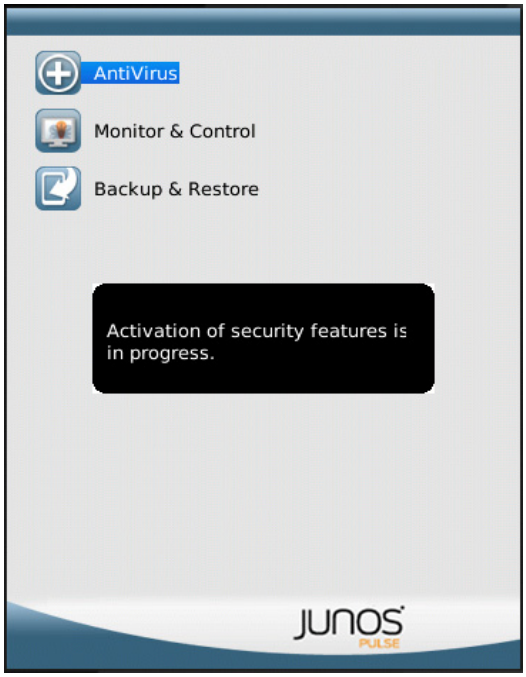
Registro de seguridad

Una vez que acepte el Acuerdo de licencia, deberá realizar el registro para obtener las funciones de seguridad. Su administrador será quien configure qué tipo de registro necesita su dispositivo: registro automático o manual.

Registro automático

Si registra el dispositivo de forma automática para obtener las funciones de seguridad, después de aceptar el Acuerdo de licencia de usuario final, se iniciará el proceso de registro inmediatamente, sin ningún tipo de solicitud. Consulte la Figura 8 en la página 9.

Figura 8: Registro automático

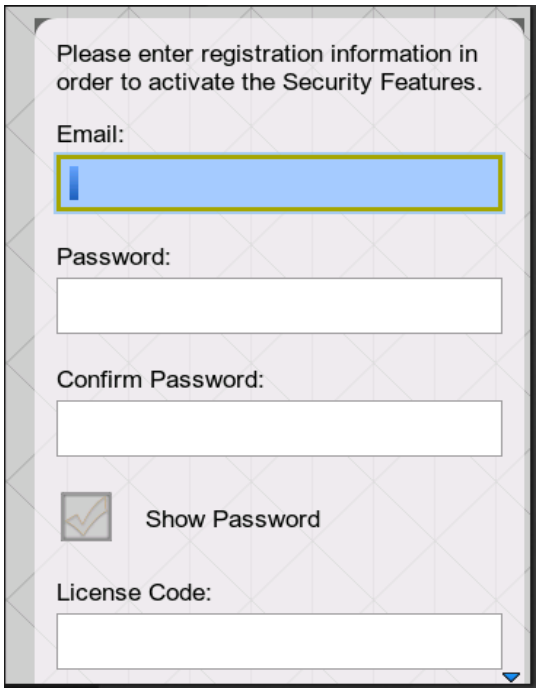


Registro manual

Si registra el dispositivo de forma manual para obtener las funciones de seguridad, después de aceptar el acuerdo de licencia de usuario final se le solicitará que haga lo siguiente:

1. Ingrese una dirección de **correo electrónico** y una **contraseña**. (La información de usuario y de contraseña no se utiliza en este momento). Consulte la Figura 9 en la página 10.
2. Vuelva a ingresar la contraseña en el campo **Confirm Password** (Confirmar contraseña).
3. Especifique el **código de licencia** que le proporcionó su administrador.
4. Ingrese su **número de teléfono** y haga clic en **Finish** (Finalizar). En algunos casos, este campo está previamente cumplimentado. Si el número no aparece, ingréselo manualmente, incluidos el código de país y el código de área sin los prefijos internacionales '00' ni '+'. No utilice espacios, paréntesis ni caracteres especiales.

Figura 9: Registro manual



Una vez que se haya instalado y registrado la aplicación, el icono de Junos Pulse aparecerá en la carpeta de aplicaciones.

Funciones disponibles de Junos Pulse

Su administrador será quien decida qué funciones de Junos Pulse tendrá a su disposición.

Junos Pulse puede incluir las funciones siguientes (consulte la Figura 6 en la página 8).

- **Antivirus (y detección de malware):** control de las actividades del antivirus y detección de malware instalado.
- **Supervisión y control:** visualización de los ajustes de supervisión.
- **Respaldar datos:** respaldo de la información del calendario y los contactos.

Copyright © 2011, Juniper Networks, Inc.

Figura 10: Funciones de Junos Pulse

Consulte “Funciones de seguridad de BlackBerry” en la página 51 para obtener información sobre las funciones y la configuración de Junos Pulse en dispositivos BlackBerry.

Instrucciones de instalación y registro para iOS

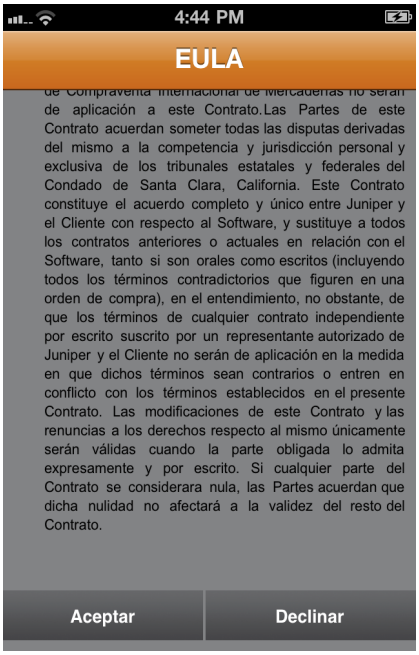
Utilice las instrucciones siguientes para descargar, instalar y registrar el software de Junos Pulse.

Las funciones de VPN de Junos Pulse y las funciones de seguridad de Junos Pulse están disponibles en la aplicación Junos Pulse, que está a su vez disponible en la tienda de aplicaciones de Apple. Las funciones de seguridad sólo están disponibles después de haber registrado el dispositivo iOS.

1. La descarga e instalación de Junos Pulse se realiza de la misma manera que la instalación de cualquier aplicación de iOS. Puede descargar Junos Pulse e importarlo a iTunes con el fin de instalarlo en su dispositivo iOS. Después de haber instalado Junos Pulse, realice lo siguiente para registrarlo automáticamente y comenzar a utilizar las funciones de VPN y de seguridad.
2. Una vez que haya descargado e instalado la aplicación, busque la URL de registro proporcionada por su administrador en un mensaje de correo electrónico o mensaje de texto.
3. Al hacer clic en la URL de registro, se mostrará el Acuerdo de licencia de usuario final de Junos Pulse. Haga clic en **Accept** (Aceptar) para continuar. Consulte la Figura 11 en la página 12.

Copyright © 2011, Juniper Networks, Inc.

Figura 11: Aceptación del Acuerdo de licencia de usuario final


4:44 PM
EULA
de aplicación a este Contrato.Las Partes de este Contrato acuerdan someter todas las disputas derivadas del mismo a la competencia y jurisdicción personal y exclusiva de los tribunales estatales y federales del Condado de Santa Clara, California. Este Contrato constituye el acuerdo completo y único entre Juniper y el Cliente con respecto al Software, y sustituye a todos los contratos anteriores o actuales en relación con el Software, tanto si son orales como escritos (incluyendo todos los términos contradictorios que figuren en una orden de compra), en el entendimiento, no obstante, de que los términos de cualquier contrato independiente por escrito suscrito por un representante autorizado de Juniper y el Cliente no serán de aplicación en la medida en que dichos términos sean contrarios o entren en conflicto con los términos establecidos en el presente Contrato. Las modificaciones de este Contrato y las renuncias a los derechos respecto al mismo únicamente serán válidas cuando la parte obligada lo admita expresamente y por escrito. Si cualquier parte del Contrato se considerara nula, las Partes acuerdan que dicha nulidad no afectará a la validez del resto del Contrato.
Aceptar
Declinar

4. A continuación, se le pedirá que habilite Junos Pulse. Haga clic en el botón Enable (Habilitar) para continuar. Consulte la Figura 12 en la página 12.

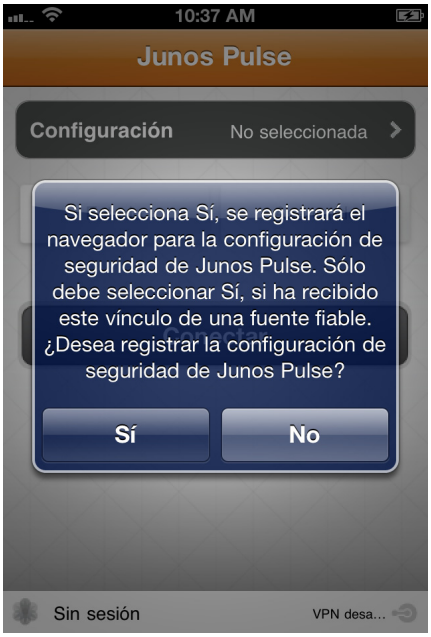
Figura 12: Habilitación de Junos Pulse

5. Después, se le solicitará que realice el registro para obtener las funciones de seguridad. Haga clic en **Yes** (Sí) para registrar las funciones de seguridad del dispositivo iOS. Consulte la Figura 13 en la página 13.

Nota informativa: si ha registrado anteriormente Junos Pulse con este dispositivo, deberá eliminar el perfil de seguridad anterior antes de poder registrar un perfil de seguridad nuevo.

Copyright © 2011, Juniper Networks, Inc.

Figura 13: Registro de seguridad


10:37 AM
Junos Pulse
Configuración
No seleccionada
Si selecciona Sí, se registrará el navegador para la configuración de seguridad de Junos Pulse. Sólo debe seleccionar Sí, si ha recibido este vínculo de una fuente fiable. ¿Desea registrar la configuración de seguridad de Junos Pulse?
Sí
No
Sin sesión
VPN desa...

6. Una vez que Junos Pulse está habilitado, se le solicitará que instale el perfil de seguridad de Junos Pulse. Haga clic en el botón **Install** (Instalar). Consulte la Figura 14 en la página 13.

Figura 14: Instalación de perfil

7. Se mostrará una pantalla que le informará de que al instalar este perfil su administrador podrá controlar y acceder de forma remota a determinados aspectos de su dispositivo. Esto es necesario para poder utilizar las funciones de seguridad, como el bloqueo remoto o la limpieza remota. Haga clic en el botón **Install** (Instalar) para continuar. Consulte la Figura 15 en la página 14.

Figura 15: Aviso de instalación de perfil

4:25 PM
Cancelar
Aviso
Instalar
Mobile Device Management
La instalación de este perfil permitirá al administrador de “https://ptest5.smobilesystems.com:8443/smobile/iportal.htm” gestionar este iPhone remotamente.
El administrador puede recopilar información personal almacenada en su iPhone, obtener la lista de aplicaciones, añadir o eliminar cuentas y restricciones y borrarlo remotamente.

Copyright © 2011, Juniper Networks, Inc.

8. Se mostrará una pantalla para indicarle que el perfil de seguridad se ha instalado correctamente. Consulte la Figura 16 en la página 15. Su dispositivo iOS tiene ahora las funciones de seguridad.

Figura 16: Perfil instalado correctamente

9. Al volver a iniciar Junos Pulse, si su administrador ha configurado los servicios de seguimiento de ubicación por GPS en su dispositivo, se le solicitará que permita el seguimiento de la ubicación por GPS utilizando su ubicación actual. Haga clic en **OK** (Aceptar) para permitir este servicio. Haga clic en **Don't Allow** (Declinar) para no permitirlo. Consulte la Figura 17 en la página 15.

Figura 17: Habilitación del seguimiento por GPS

Nota informativa: si su dispositivo iOS no tiene los servicios de ubicación activados, se mostrará la solicitud siguiente (consulte la Figura 18 en la página 16):

Figura 18: Activación de los servicios de ubicación

Nota informativa: haga clic en el botón Settings (Ajustes) (consulte la Figura 18 en la página 16) para acceder a la pantalla de servicios de ubicación en la que podrá activar estos servicios. A continuación, deberá volver a iniciar Junos Pulse para habilitar el informe de seguimiento por GPS.

Precaución: una vez que haya permitido o no la activación de los servicios de seguimiento por GPS, se recordará esta selección si desinstala y vuelve a instalar Junos Pulse. No se le solicitará que realice la selección otra vez; se utilizará la selección anterior. Si desea restablecer esta función para cambiar la selección, en el dispositivo iOS, vaya a Settings (Ajustes) > General > Reset Location Warnings (Restablecer avisos de ubicación). Esto restablecerá todos los avisos de ubicación para todas las aplicaciones.

Instrucciones de instalación y registro para Windows Mobile

Utilice las instrucciones siguientes para descargar, instalar y registrar el software de Junos Pulse.

1. Por medio del navegador Web de Windows Mobile, descargue el software de Junos Pulse directamente en el dispositivo.

   Al descargar la aplicación en el dispositivo, se mostrará el archivo .CAB en la carpeta Archivos de programa del dispositivo.

2. Para comenzar la instalación, busque el archivo .CAB de instalación con el **explorador de archivos**, al que podrá acceder desde el menú **Inicio**.

Copyright © 2011, Juniper Networks, Inc.

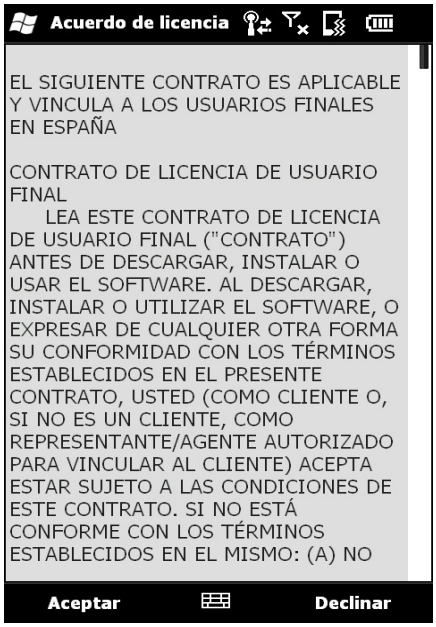
3. Seleccione el archivo **.CAB** y responda a la solicitud para especificar la ubicación en la que desea guardar la aplicación, **Store to device** (Almacenar en dispositivo) o **Store to memory card** (Almacenar en tarjeta de memoria).

   Después de instalar Junos Pulse, debe reiniciar el teléfono para que funcione la aplicación de cortafuegos. Cuando esté instalado, el icono de **Junos Pulse** aparece en el menú **Inicio** y en la lista **Programas**.

4. A continuación, comenzará el proceso de registro. Seleccione el icono de la aplicación **Junos Pulse**.

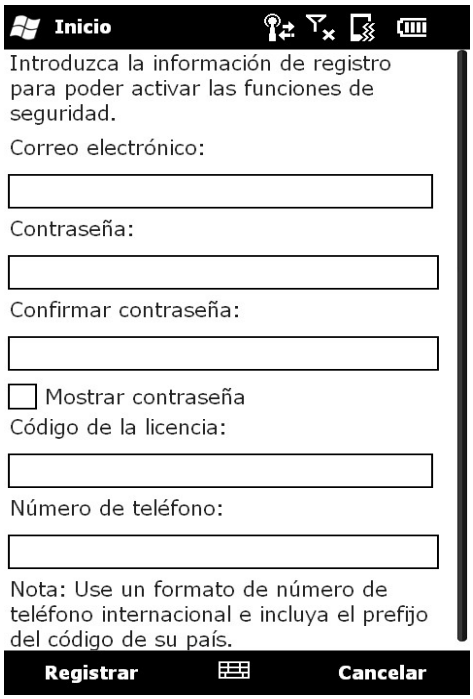
5. A continuación, deberá aceptar el acuerdo de licencia (consulte la Figura 19 en la página 17). Seleccione **Accept** (Aceptar) para pasar a la pantalla de registro.

Figura 19: Acuerdo de licencia de Junos Pulse


Acuerdo de licencia
EL SIGUIENTE CONTRATO ES APLICABLE Y VINCULA A LOS USUARIOS FINALES EN ESPAÑA
CONTRATO DE LICENCIA DE USUARIO FINAL
LEA ESTE CONTRATO DE LICENCIA DE USUARIO FINAL ("CONTRATO") ANTES DE DESCARGAR, INSTALAR O USAR EL SOFTWARE. AL DESCARGAR, INSTALAR O UTILIZAR EL SOFTWARE, O EXPRESAR DE CUALQUIER OTRA FORMA SU CONFORMIDAD CON LOS TÉRMINOS ESTABLECIDOS EN EL PRESENTE CONTRATO, USTED (COMO CLIENTE O, SI NO ES UN CLIENTE, COMO REPRESENTANTE/AGENTE AUTORIZADO PARA VINCULAR AL CLIENTE) ACEPTA ESTAR SUJETO A LAS CONDICIONES DE ESTE CONTRATO. SI NO ESTÁ CONFORME CON LOS TÉRMINOS ESTABLECIDOS EN EL MISMO: (A) NO
Aceptar
Declinar

6. En la pantalla **Registration** (Registro), ingrese la información siguiente (consulte laFigura 20 en la página 18).
   - Ingrese su dirección de **correo electrónico**.
   - Ingrese su **contraseña** y **confírmela**. Esta contraseña debe tener al menos 6 caracteres.
   - Especifique el **código de licencia** que recibió cuando compró el producto.
   - Ingrese el **número de teléfono**, incluido el código del país.

Figura 20: Registro para Windows Mobile


Inicio
Introduzca la información de registro para poder activar las funciones de seguridad.
Correo electrónico:
Contraseña:
Confirmar contraseña:
Mostrar contraseña
Código de la licencia:
Número de teléfono:
Nota: Use un formato de número de teléfono internacional e incluya el prefijo del código de su país.
Registrar
Cancelar

7. Para finalizar el registro, seleccione **Register** (Registrar). El proceso de registro puede tardar algunos minutos.
8. Cuando el dispositivo esté registrado, se mostrará una ventana para indicarle que el registro se ha realizado correctamente. Haga clic en **OK** (Aceptar) en dicha ventana para continuar.
9. Cuando el registro se haya realizado correctamente, puede ejecutar la aplicación seleccionando el icono de **Junos Pulse** en la lista **Programas**.

   Al abrir la aplicación, podrá ver las funciones siguientes (consulte la Figura 21 en la página 19):

   - Conexión le permite agregar, editar y eliminar conexiones de red.
   - Intranet proporciona vínculos web configurados por el administrador de red.
   - Correo electrónico inicia la aplicación de correo electrónico.
   - Seguridad ofrece acceso a las funciones de seguridad siguientes:
     - Antispam protege su dispositivo frente a llamadas no solicitadas y SMS de spam.
     - Antivirus ofrece funciones de análisis para proteger los datos del dispositivo frente a malware.
     - Las funciones del cortafuegos le permiten bloquear o permitir el tráfico de datos hacia o desde el dispositivo usando listas de reglas que controlan el tráfico en base al número de puerto, dirección IP y otras opciones.

Copyright © 2011, Juniper Networks, Inc.

  - Supervisar y controlar refleja los ajustes que ha elegido (o los predeterminados) para supervisar las actividades móviles desde el panel. Los ajustes predeterminados pueden habilitar todas las funciones de supervisión: mensajes de texto, llamadas, correo electrónico y fotografías.
  - Respaldar datos respalda la información de citas del calendario y los contactos en el panel desde el dispositivo.
- Estado le permite ver, eliminar y enviar por correo electrónico los archivos de registro de Junos Pulse, lo que puede ser necesario para operaciones de solución de problemas. Los archivos de registro le muestran todos los incidentes de seguridad, como las horas de análisis para detección de virus y los virus descubiertos.
- Acerca de ofrece información sobre la versión del software de Junos Pulse.

Figura 21: Pantalla principal de Junos Pulse

Consulte “Funciones de seguridad de Windows Mobile” en la página 61 para obtener información sobre las funciones y la configuración de Junos Pulse en dispositivos Windows Mobile.

Copyright © 2011, Juniper Networks, Inc.

Capítulo 4

Utilización del panel de Mobile Security

Este capítulo describe cómo acceder y utilizar el panel de Mobile Security de Junos Pulse para configurar la supervisión y las funciones de seguridad de los dispositivos registrados.

Información general

Una vez que la aplicación Junos Pulse se ha instalado en el dispositivo y se han creado la dirección de correo electrónico y la contraseña como parte del proceso de registro e instalación del dispositivo, podrá utilizar esta dirección de correo electrónico y contraseña para iniciar sesión en el panel. Puede acceder al panel ingresando la URL que recibió de su proveedor de servicios. Consulte la Figura 22 en la página 21.

Figura 22: Ventana de inicio de sesión en el panel de Mobile Security

Una vez que haya iniciado sesión, se mostrará la ficha Inicio. Consulte la Figura 23 en la página 22. Al lado de la ficha Inicio, verá varias fichas para cada área funcional del panel. Estas fichas son las siguientes:

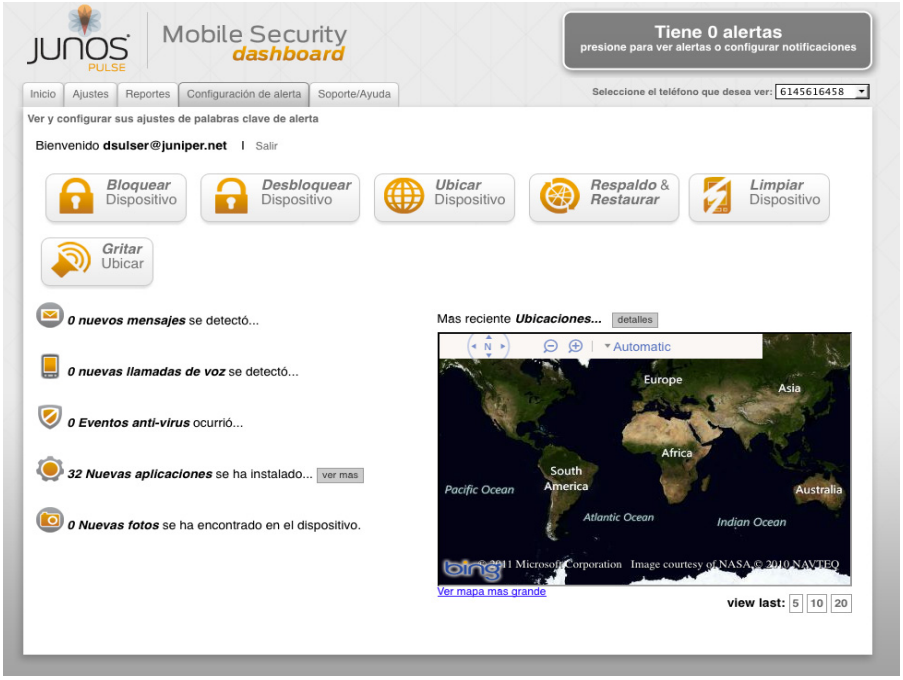
- Inicio: ofrece enlaces a mensajes y llamadas registrados, virus encontrados, aplicaciones instaladas y fotografías. También informa sobre ubicaciones recientes por GPS.
- Ajustes: configure cuentas de usuario y dispositivos diferentes que desee supervisar.

Copyright © 2011, Juniper Networks, Inc.

- Reportes: busque remitentes o palabras clave en un rango de mensajes, en base a fechas.
- Configuración de alerta: configure los parámetros para iniciar las alertas. (También puede encontrar el estado de las alertas y configurarlas haciendo clic en el botón Alerta de la esquina superior derecha de la ventana del panel).

Nota informativa: tenga en cuenta que los ajustes de alertas no están disponibles en los dispositivos iOS.

Figura 23: Ficha Inicio



Comandos y eventos de la ficha Inicio

Desde la ficha Inicio puede enviar comandos y acceder a los eventos del dispositivo de la manera siguiente:

Comandos

Haga clic en cualquiera de los botones siguientes para enviar el comando en cuestión. Al hacer clic en un botón de comando, se muestra una ventana que le solicita que confirme el comando que ha elegido antes de que se envíe.

Nota informativa: los comandos para los dispositivos iOS son diferentes. Consulte “Comandos para los dispositivos iOS” en la página23.

- **Lock Device** (Bloquear dispositivo): bloquea el dispositivo en caso de pérdida o robo, o en caso de que desee que el dispositivo deje de funcionar por algún otro motivo.
- **Unlock Device** (Desbloquear dispositivo): desbloquea el dispositivo.
- **Locate Device** (Ubicar dispositivo): envía un comando para determinar la ubicación del dispositivo por GPS y el resultado se muestra en un mapa de la ficha Inicio.
- **Backup and Restore** (Respaldo y restaurar): crea una copia de la información del calendario y los contactos. Esto resulta útil en caso de pérdida o robo del dispositivo.

Copyright © 2011, Juniper Networks, Inc.

- **Wipe Device** (Limpiar dispositivo): elimina los datos personales del dispositivo, como contactos, eventos del calendario, notas, historial de llamadas, carpetas de mensajes, y todos los datos de la tarjeta SD.
- **Scream Locate** (Gritar ubicar): permite al usuario del dispositivo ubicar el dispositivo a una distancia audible mediante la emisión de un sonido, incluso si se han silenciado el altavoz y el timbre.

Comandos para los dispositivos iOS

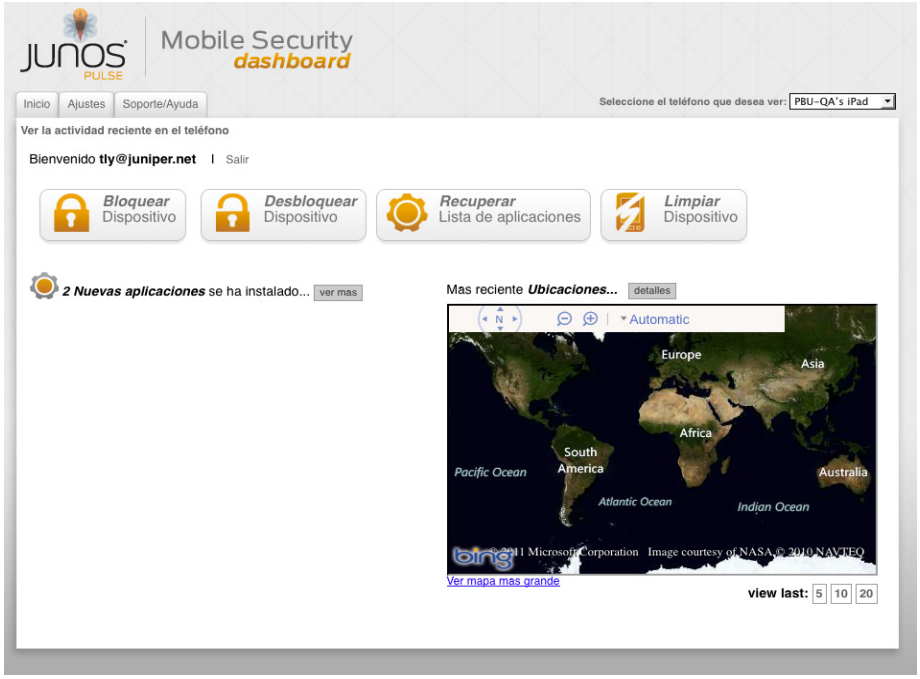
Para los dispositivos iOS, los comandos disponibles en la ficha Inicio son los siguientes (consulte la Figura 24 en la página 23):

- **Lock Device** (Bloquear dispositivo): bloquea el dispositivo en caso de pérdida o robo, o en caso de que desee que el dispositivo deje de funcionar por algún otro motivo.
- **Unlock Device** (Desbloquear dispositivo): desbloquea el dispositivo.
- **Retrieve App List** (Recuperar lista de aplicaciones): actualiza la lista de aplicaciones instaladas en el dispositivo.
- **Wipe Device** (Limpiar dispositivo): elimina los datos personales del dispositivo, como contactos, eventos del calendario, notas, historial de llamadas, carpetas de mensajes, y todos los datos de la tarjeta SD.

Nota informativa: no existen comandos disponibles para los dispositivos iOS que no tengan asociado un certificado APNS. Si no existe un certificado APNS, la ubicación por GPS es la única función disponible.

Nota informativa: la función GPS no se admite en el dispositivo iPod Touch ni en los dispositivos iOS que no tengan un servicio celular.

Figura 24: Ficha Inicio para dispositivos iOS



Eventos

Cuando existen eventos para cualquiera de las categorías enumeradas, podrá verse un botón que permita **visualizar más**. Consulte la Figura 23 en la página 22. Puede eliminar elementos de las categorías de eventos (mensajes, llamadas de voz, etc.) desde el panel cuando haga clic en **View more (Visualizar más)**. En la ventana que se muestre, seleccione la casilla de verificación al lado del elemento que desea eliminar y haga clic en el botón **Delete** (Eliminar). También puede hacer clic en el botón **Select All** (Seleccionar todos) y, a continuación, en el botón **Delete** (Eliminar) para eliminar todos los elementos de esa categoría de eventos.

Nota informativa: los dispositivos iOS tienen eventos diferentes. Consulte “Eventos para dispositivos iOS” en la página25.

- **Mensajes:** vea los mensajes (voz, correo electrónico, texto) que se han recibido en el dispositivo.

  Haga clic en **View more** (Visualizar más) (si está disponible) para ver todos los mensajes de la lista. Consulte la Figura 25 en la página 25.

- **Llamadas de voz:** vea las llamadas de voz recibidas en el dispositivo.

  Haga clic en **View more** (Visualizar más) (si está disponible) para ver todas las llamadas de la lista.

- **Eventos de antivirus:** vea los nuevos eventos de antivirus que se han producido.

  Haga clic en **View more** (Visualizar más) (si está disponible) para ver todos los virus detectados.

- **Aplicaciones nuevas:** vea las nuevas aplicaciones que se han instalado en el dispositivo.

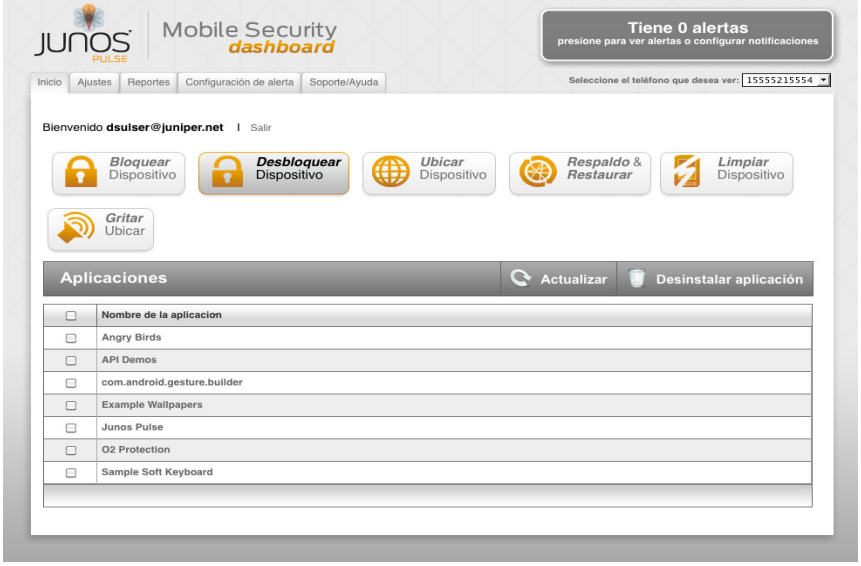
  Haga clic en **View more** (Visualizar más) (si está disponible) para abrir una ventana nueva que enumere las aplicaciones instaladas recientemente. Puede desinstalar una aplicación de forma remota seleccionando la casilla de verificación que se encuentra al lado de la aplicación y haciendo clic en el botón **Uninstall specific application on the handset** (Desinstalar la aplicación específica en el teléfono).

- **Fotografías nuevas**: vea las nuevas fotografías almacenadas en el dispositivo.

  Haga clic en **View more** (Visualizar más) (si está disponible) para abrir una ventana nueva que muestre las fotografías (20 imágenes por pantalla).

Copyright © 2011, Juniper Networks, Inc.

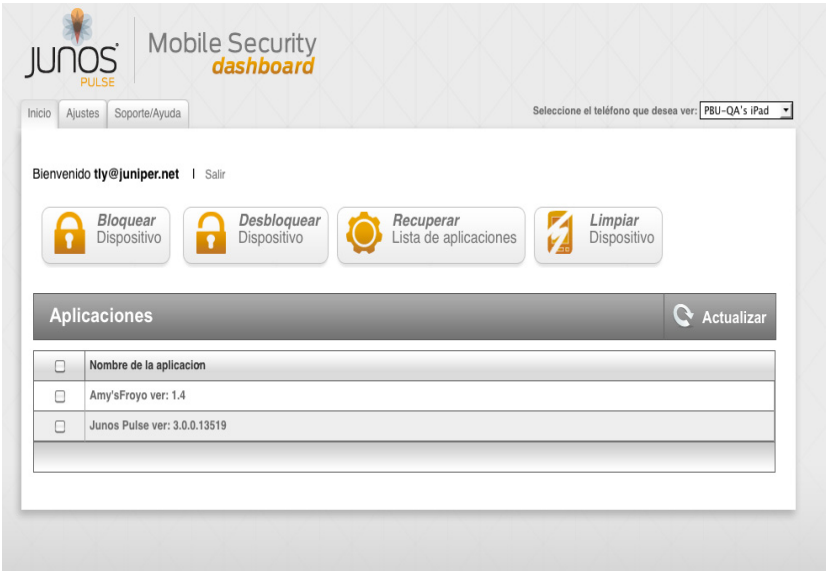
Figura 25: Ventana View more (Visualizar más) de eventos de mensajes detectados



Eventos para dispositivos iOS

Aplicaciones nuevas es el único evento disponible para iOS de momento. Haga clic en **View more** (Visualizar más) (si está disponible) para abrir una ventana nueva que enumere las aplicaciones instaladas recientemente (consulta la Figura 26 en la página 25).

Figura 26: Ventana View more (Visualizar más) de eventos de instalación de aplicaciones detectados



Copyright © 2011, Juniper Networks, Inc.

Información y configuración de la ficha Ajustes

En la ficha Ajustes, puede configurar la administración de la cuenta y la administración del teléfono. Consulte la Figura 27 en la página 28. Por ejemplo, puede modificar la dirección de correo electrónico a la que se envían las alertas.

Administración de cuentas

Puede eliminar, editar o agregar una dirección de correo electrónico nueva a la cuenta de un dispositivo.

Para agregar una dirección de correo electrónico y la contraseña correspondiente:

1. Seleccione la ficha **Settings** (Ajustes).
2. En la lista desplegable **Select phone to view** (Sellecione el teléfono que desea ver) de la esquina superior derecha, seleccione el dispositivo que desea administrar.
3. Para agregar una dirección de correo electrónico nueva para la administración de la cuenta del teléfono, ingrese la dirección de correo electrónico en el campo de edición **Nombre de usuario (correo electrónico)**.
4. Ingrese la contraseña nueva en el campo de edición **Password** (Contraseña).
5. Haga clic en el botón **Add User** (Agregar usuario).

Para eliminar una dirección, selecciónela y haga clic en **Remove Selected** (Eliminar la selección).

Para editar una dirección, realice la edición en el campo destinado a tal fin y haga clic en **Update Email** (Actualizar correo electrónico). Es importante tener en cuenta que al cambiar esta dirección también se cambia el nombre de usuario de inicio de sesión para la cuenta.

Administración del teléfono

Con la administración del teléfono puede actualizar las funciones de supervisión específicas del dispositivo, cambiar el período de actualización del GPS, controlar los límites de tamaño de los archivos de registro y determinar los parámetros de limpieza de datos. Tenga en cuenta que las actualizaciones no se reciben hasta que el dispositivo vuelva a enviar informes según la planificación.

Nota informativa: la administración del teléfono no está disponible en los dispositivos iOS. En la ficha Ajustes, puede ver la información del teléfono para el dispositivo iOS seleccionado, como el número de teléfono, tipo de dispositivo, nombre del dispositivo y UDID. Consulte la Figura 28 en la página 28.

Para actualizar o modificar los ajustes disponibles, realice lo siguiente:

1. Si no lo ha seleccionado todavía, en la lista desplegable **Select phone to view** (Seleccione el teléfono que desea ver) de la esquina superior derecha, seleccione el número de teléfono para el dispositivo que desee administrar.

   En la columna **Handset Management** (Administración del teléfono) de la parte derecha de la ventana, realice lo siguiente:
2. Al lado de **Supervisión de correo electrónico**, seleccione la casilla de verificación para habilitar esta función para el dispositivo seleccionado.
3. Al lado de **Supervisión de SMS** (servicio de mensajes breves), seleccione la casilla de verificación para habilitar la supervisión de mensajes para el dispositivo seleccionado.

Copyright © 2011, Juniper Networks, Inc.

4. Al lado de **Supervisión de MMS** (servicio de mensajes multimedia), seleccione la casilla de verificación para habilitar la supervisión de mensajes que contengan imágenes, vídeos, sonido u otro tipo de contenido multimedia para el dispositivo seleccionado.
5. Al lado de **Supervisión de voz**, seleccione la casilla de verificación para habilitar esta función para el dispositivo seleccionado. Supervisión de voz ofrece una marca de hora para una conversación.
6. Al lado de **Registrar límites de eventos**, seleccione un límite de eventos disponible en la lista desplegable. Le recomendamos que no establezca el límite por debajo de 25.
7. Al lado de **Registrar límites de tamaño**, seleccione un límite de tamaño disponible en la lista desplegable. Le recomendamos que no establezca el límite en Desactivado.

   Las opciones Log Event Limit (Registrar límites de eventos) y Log Size Limit (Registrar límites de tamaño) funcionan en consonancia, teniendo efecto la primera en activarse. El límite de eventos hace que el dispositivo envíe la cantidad de eventos especificada (correo electrónico, voz, SMS, MMS) como un evento combinado cuando se llegue al límite del evento. Esto es preferible a enviar cada evento individual en tiempo real. Si el dispositivo envía o recibe una gran cantidad de mensajes, deberá establecer este límite con un valor alto en vez de bajo. Si no lo hace, el dispositivo podría estar enviando eventos constantemente al panel, lo que podría obstaculizar el rendimiento del dispositivo. La opción Log Size Limit (Registrar límites de tamaño) restringe la cantidad de datos supervisados que se envían desde el dispositivo. El límite que se consigue primero es el que se utiliza.
8. Al lado de **Supervisión de imagen**, seleccione la casilla de verificación para habilitar esta función para el dispositivo seleccionado.
9. Al lado de **Supervisión de imágenes Web**, seleccione la casilla de verificación para habilitar esta función para el dispositivo seleccionado.
10. Al lado de **Período de actualización de GPS**, seleccione un margen de tiempo de actualización disponible en la lista desplegable. Con este ajuste, puede configurar las actualizaciones de GPS para que se lleven a cabo automáticamente cada 15 minutos, 30 minutos, cada hora o a diario.
11. Al lado de **Bloquear al cambiar SIM**, seleccione la casilla de verificación para habilitar esta función. Cuando esta función está seleccionada, si se extrae la tarjeta SIM, el dispositivo activa el GPS por robo y bloquea el dispositivo. Puede desbloquear el dispositivo con un nombre de usuario y contraseña.
12. Al lado de **Limpiar al cambiar SIM**, seleccione la casilla de verificación para habilitar esta función. Esta casilla de verificación sólo está disponible cuando la casilla de verificación Lock on SIM Change (Bloquear al cambiar SIM) está habilitada. Con esta función seleccionada, si la tarjeta SIM se cambia por otra, el dispositivo realiza todas las acciones de Lock on SIM Change (Bloquear al cambiar SIM) y elimina la información confidencial del dispositivo.
13. Haga clic en el botón **Update** (Actualizar) para aplicar todos los ajustes.

Copyright © 2011, Juniper Networks, Inc.

Figura 27: Ficha Ajustes

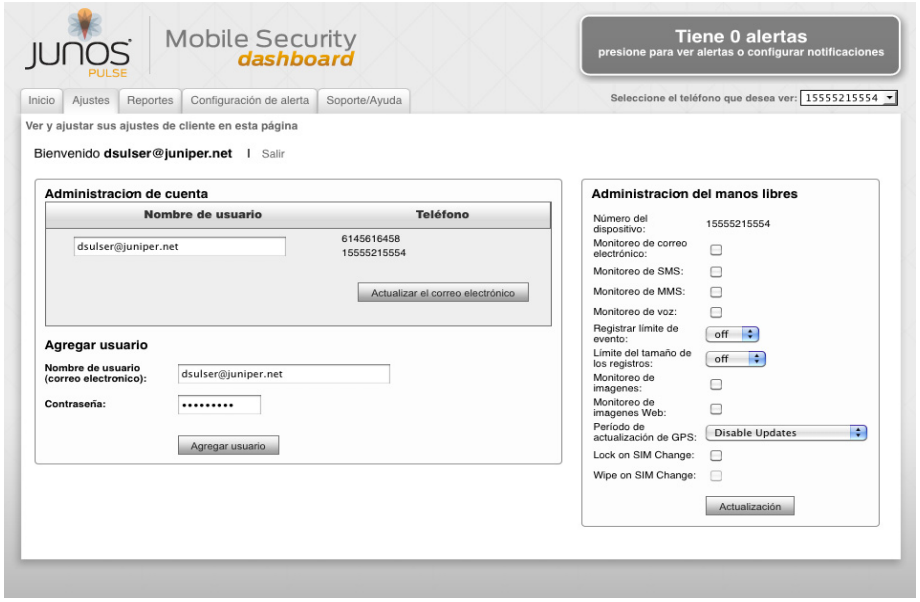
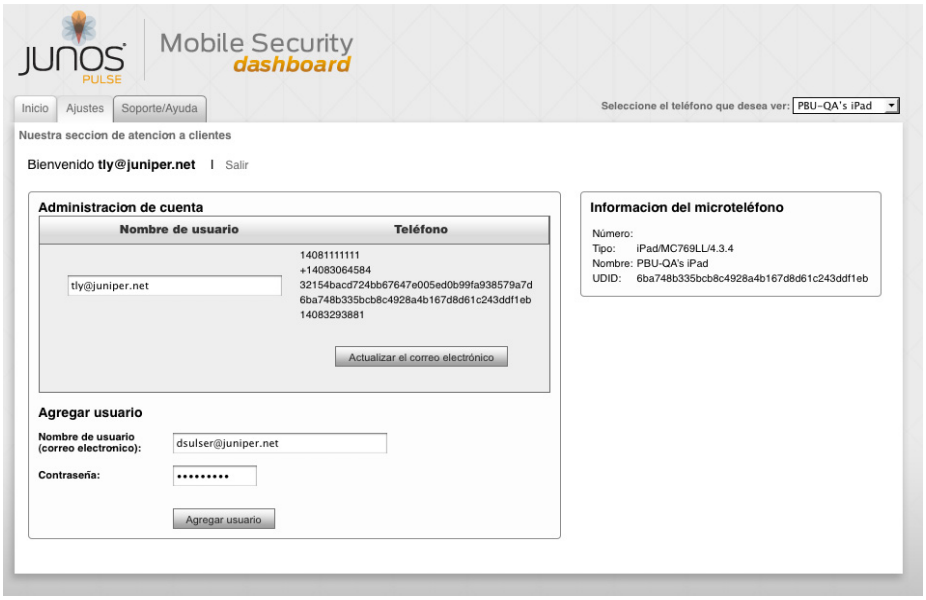


Figura 28: Ficha Ajustes para dispositivos iOS



Copyright © 2011, Juniper Networks, Inc.

Información y configuración de la ficha Reportes

Puede realizar informes personalizados con los datos recopilados del dispositivo ingresando diferentes criterios en los campos proporcionados en esta ventana.

Para realizar un informe personalizado, ingrese los criterios del informe en uno o más de los campos descritos aquí.

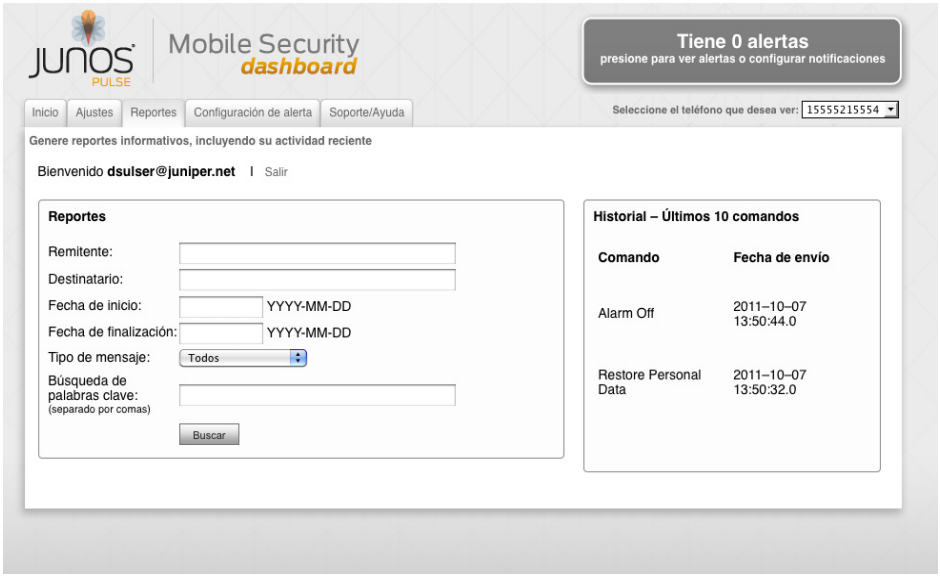
1. Seleccione la ficha **Reports** (Reportes). Consulte la Figura 29 en la página 30.
2. Si no lo ha seleccionado todavía, en la lista desplegable **Select phone to view** (Seleccione el teléfono que desea ver) de la esquina superior derecha, seleccione el número de teléfono para el dispositivo para el que desee crear un informe.
3. Si desea que el informe incluya información del remitente, ingrese la dirección de correo electrónico del **remitente** o su número de teléfono en el campo correspondiente. Tenga en cuenta que la dirección o el número que ingrese deben coincidir con la dirección o número del remitente que aparece en la pantalla de mensajes.
4. Si desea que el informe incluya información del destinatario, ingrese la dirección de correo electrónico del **destinatario** o su número de teléfono en el campo correspondiente. Tenga en cuenta que la dirección o el número que ingrese deben coincidir con la dirección o número del destinatario que aparece en la pantalla de mensajes.
5. En el campo **Start Date** (Fecha de inicio), ingrese un parámetro de fecha de inicio para el informe que está creando. El formato de la fecha deberá ser Año-Mes-Día, como en el ejemplo siguiente: 2010-11-24.
6. En el campo **End Date** (Fecha de finalización), ingrese un parámetro de fecha de finalización para el informe que está creando. El formato de la fecha deberá ser Año-Mes-Día, como en el ejemplo siguiente: 2010-11-24.
7. En la lista desplegable **Messages** (Mensajes), seleccione el tipo de mensaje para el que está ejecutando este informe. Las opciones son Todos, SMS, MMS, Correo electrónico, Voz.
8. En el campo de edición **Keyword Search** (Búsqueda de palabras clave), ingrese una palabra clave o frase que desee buscar en los mensajes. Los mensajes en los que aparece esta palabra se utilizarán para crear su informe.
9. Haga clic en el botón **Search** (Buscar) para ejecutar el informe.

Copyright © 2011, Juniper Networks, Inc.

Historial

En la parte derecha de la ventana de Reportes, existe una columna llamada **Historial**. Aquí puede ver los últimos diez comandos enviados al dispositivo y las fechas de envío.

Figura 29: Ficha Reportes



Información y configuración de la ficha Configuración de alerta

Al utilizar identificadores únicos, como palabras clave o direcciones, los mensajes que cumplen un criterio definido pueden identificarse y visualizarse haciendo clic en la casilla **Alerts (Alertas)** que se encuentra en la esquina superior derecha del panel. Las alertas también pueden configurarse para que las reciba por correo electrónico; por ejemplo, puede recibir automáticamente por correo electrónico un mensaje SMS que tenga una palabra clave que haya designado.

Para configurar una alerta, realice lo siguiente.

1. Seleccione la ficha **Alert Setup** (Configuración de alerta). Consulte la Figura 30 en la página 31.
2. Si no lo ha seleccionado todavía, en la lista desplegable **Select phone to view** (Seleccione el teléfono que desea ver) de la esquina superior derecha, seleccione el número de teléfono para el dispositivo para el que desee configurar una alerta.
3. En el campo de edición **Add Keyword** (Agregar palabra clave), ingrese la palabra clave que desea que accione la alerta si dicha palabra se encuentra en un mensaje enviado desde el dispositivo o recibido en él. Haga clic en el botón **Add** (Agregar). La palabra clave aparece ahora en la lista de palabras clave en el siguiente campo.

Copyright © 2011, Juniper Networks, Inc.

4. El campo **Keywords** (Palabras clave) tiene también una **casilla de verificación** que le permite utilizar palabras clave sugeridas de la columna del lado derecho de la ventana. Estas son palabras clave que se utilizan a menudo como mensajes abreviados. Para utilizar palabras clave sugeridas en lugar de, o además de, las palabras clave que ingrese, seleccione la casilla de verificación **Use Suggested Keywords** (Utilizar palabras clave sugeridas). Cuando esta casilla de verificación se ha seleccionado, las palabras clave sugeridas que se han habilitado se utilizarán como parte de la alerta.

   Puede desplazarse por la lista de palabras clave sugeridas y habilitar casillas de verificación al lado de las palabras clave que desee que activen una alerta en el caso de encontrarse en los mensajes.

5. Si selecciona **Send the event as an Email Message** (Enviar el evento como mensaje de correo electrónico) habilitando la casilla de verificación del campo **Sender/Recipient Address** (Dirección del remitente/destinatario), ingrese la dirección de correo electrónico o número de teléfono para comprobar si hay alertas. Utilice esta función para señalar como alerta cualquier comunicación con un contacto particular.

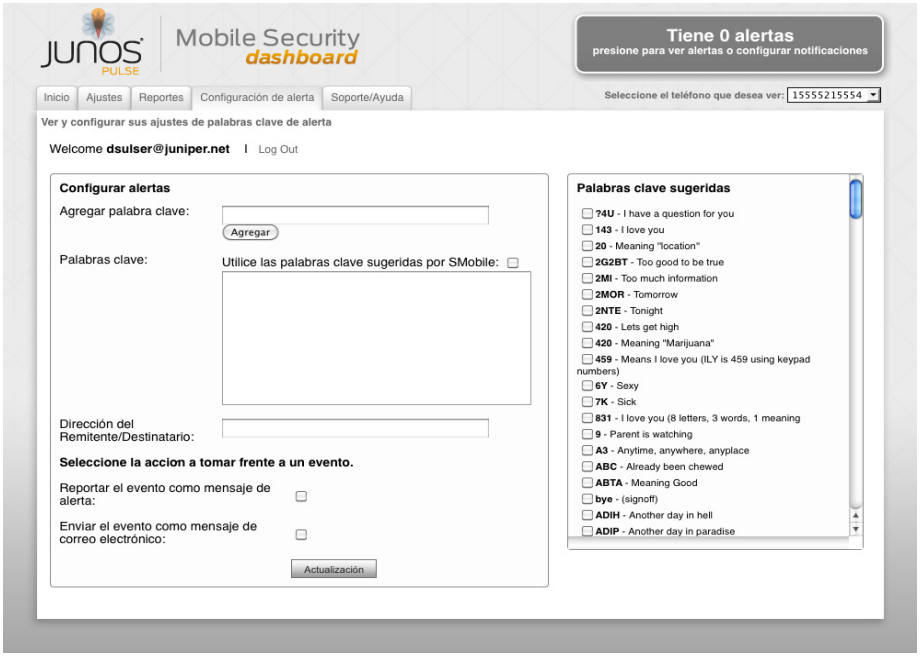
6. En las opciones **Select what to do with an event** (Seleccionar la acción a seguir con un evento), puede elegir lo siguiente:

   - **Report the event as an Alert message** (Informar del evento como mensaje de alerta)
   - **Send the event as an Email message** (Enviar el evento como mensaje de correo electrónico)

   Seleccionar una o ambas casillas de verificación.

7. Haga clic en el botón **Update** (Actualizar) para habilitar la alerta.

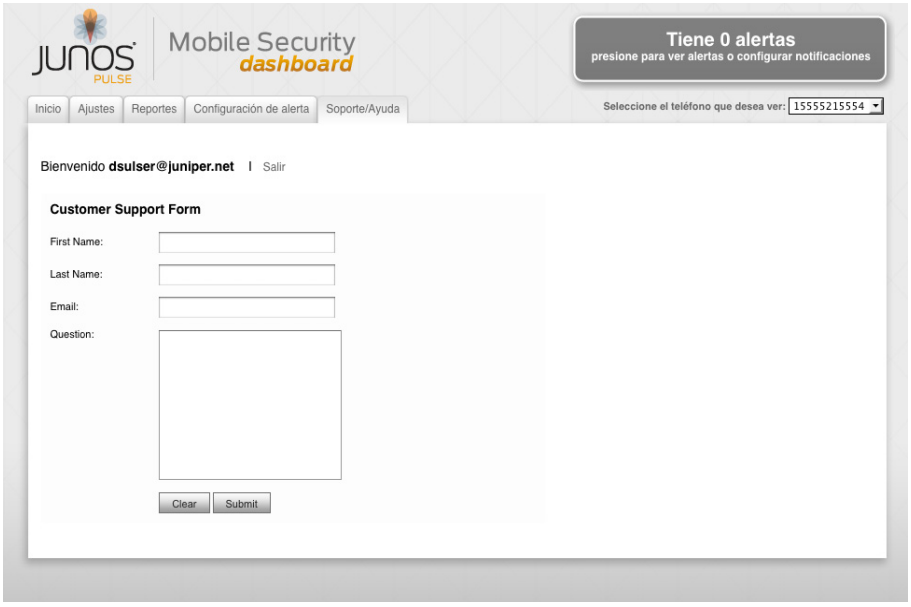
Figura 30: Ficha Configuración de alerta


JUNOS PULSE
Mobile Security dashboard
Tiene 0 alertas
presione para ver alertas o configurar notificaciones
Inicio
Ajustes
Reportes
Configuración de alerta
Soporte/Ayuda
Seleccione el teléfono que desea ver: 15555215554
Ver y configurar sus ajustes de palabras clave de alerta
Welcome dsulser@juniper.net | Log Out
Configurar alertas
Agregar palabra clave:
Agregar
Palabras clave:
Utilice las palabras clave sugeridas por SMobile:
Dirección del Remitente/Destinatario:
Seleccione la accion a tomar frente a un evento.
Reportar el evento como mensaje de alerta:
Enviar el evento como mensaje de correo electrónico:
Actualización
Palabras clave sugeridas
?4U - I have a question for you
143 - I love you
20 - Meaning "location"
2G2BT - Too good to be true
2MI - Too much information
2MOR - Tomorrow
2NTE - Tonight
420 - Lets get high
420 - Meaning "Marijuana"
459 - Means I love you (ILY is 459 using keypad numbers)
6Y - Sexy
7K - Sick
831 - I love you (8 letters, 3 words, 1 meaning
9 - Parent is watching
A3 - Anytime, anywhere, anyplace
ABC - Already been chewed
ABTA - Meaning Good
bye - (signoff)
ADIH - Another day in hell
ADIP - Another day in paradise

Información y configuración de la ficha Soporte/Ayuda

Si tiene alguna pregunta o necesita soporte técnico, seleccione la ficha **Support/Help** (Soporte/Ayuda). Ingrese la información necesaria en los campos disponibles y haga clic en **Submit** (Enviar).

Figura 31: Ficha Soporte/Ayuda



Copyright © 2011, Juniper Networks, Inc.

Capítulo 5

Utilización de Junos Pulse en los dispositivos móviles

Este capítulo describe las funciones de seguridad y conexión disponibles en cada dispositivo admitido.

Funciones de seguridad en Android

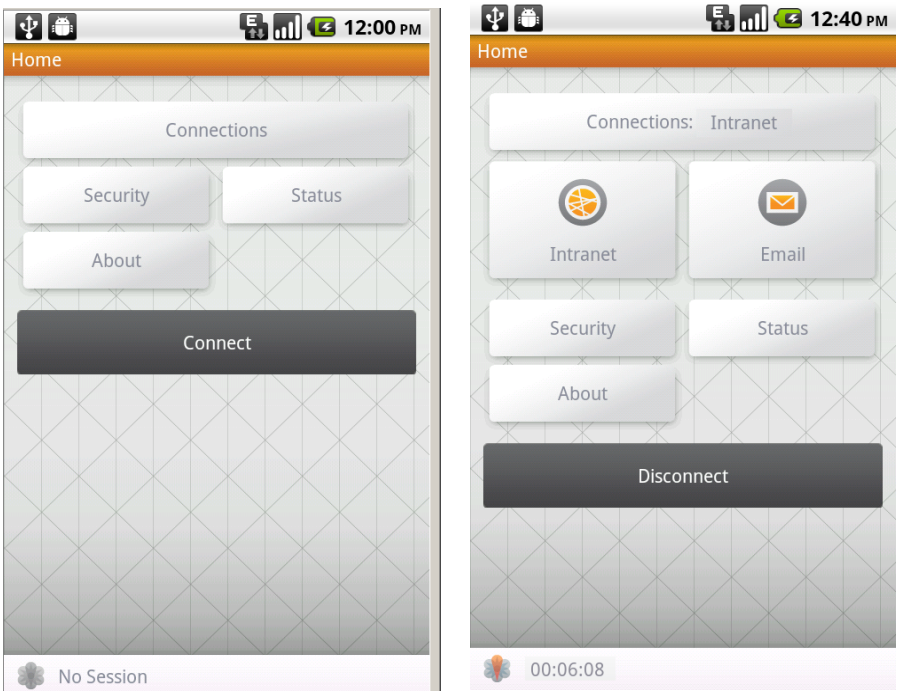
Su administrador será quien decida qué funciones de Junos Pulse tendrá a su disposición. Es posible que pueda ver más funciones una vez que establezca una conexión con la red. (Consulte “Adición de una conexión segura” en la página 35 para ver las instrucciones).

Junos Pulse puede incluir las funciones siguientes (consulte la Figura 32 en la página 34).

- **Conexiones:** le permite agregar, editar y eliminar conexiones de red corporativas.
- **Intranet:** proporciona vínculos Web configurados por su administrador.
- **Correo electrónico:** inicia la aplicación de correo electrónico.
- **Seguridad:** ofrece acceso a las funciones de seguridad.
- **Estado:** le permite ver, eliminar y enviar por correo electrónico los archivos de registro, lo que puede ser necesario para operaciones de solución de problemas. Los archivos de registro le muestran todos los incidentes de seguridad, como las horas de análisis para detección de virus y los virus descubiertos. Si cuenta con una conexión VPN establecida, también podrá ver el estado de dicha conexión en esta pantalla.
- **Acerca de:** ofrece información sobre la versión del software.

Copyright © 2011, Juniper Networks, Inc.

Figura 32: Funciones disponibles

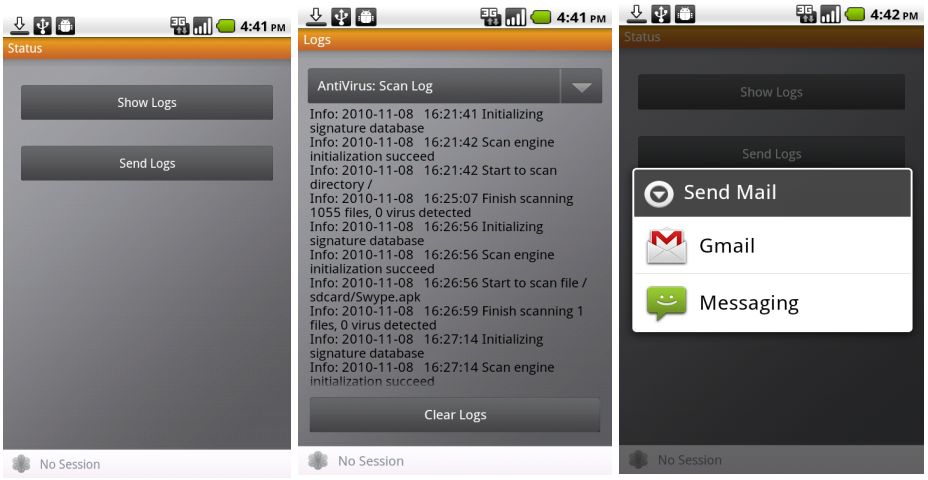


Estado

Seleccione el icono de **Junos Pulse** de la carpeta **Applications** (Aplicaciones) para acceder a las funciones de Pulse disponibles para su dispositivo. Seleccione **Status** (Estado) para ver y enviar los archivos de registro. Consulte la Figura 33 en la página 34.

- En la ventana **Status** (Estado) puede ver, eliminar y enviar por correo electrónico los archivos de registro, lo que puede ser necesario para operaciones de solución de problemas. Los archivos de registro le muestran todos los incidentes de seguridad, como las horas de análisis para detección de virus y los virus descubiertos. Si cuenta con una conexión VPN establecida, también podrá ver el estado de dicha conexión en esta pantalla.
- En la ventana **Status** (Estado), haga clic en **Send Logs** (Enviar registros) para enviar los registros por correo electrónico o SMS.

Figura 33: Ventana de estado de Junos Pulse en Android, visualización de registros y envío de registros



Copyright © 2011, Juniper Networks, Inc.

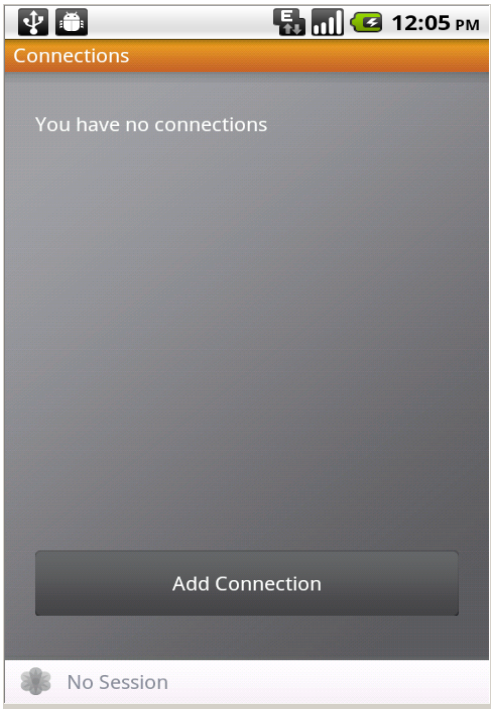
Adición de una conexión segura

Junos Pulse usa la conectividad 3G, 4G, Edge o WIFI de su dispositivo para establecer una conexión autenticada con una red protegida. Puede agregar una conexión para cada red diferente a la que se conecte. Esta es una conexión VPN segura a su red corporativa.

Para definir una conexión, realice lo siguiente:

1. Inicie Junos Pulse.
2. Seleccione **Connections** (Conexiones) (consulte la Figura 32 en la página 34).
3. Seleccione **Add Connection** (Agregar conexión) (consulte la Figura 34 en la página 35).

Figura 34: Adición de una conexión



4. Ingrese las propiedades de la conexión de la manera siguiente (consulte la Figura 35 en la página 36):
   - **Connection name** (Nombre de la conexión): un nombre descriptivo.
   - **URL:** la dirección Web proporcionada por el administrador de red.
   - **Uses Certificate** (Usa certificado): seleccione esta casilla de verificación si su administrador le ha proporcionado un certificado digital. Si no usa un certificado, debe proporcionar un nombre de usuario y contraseña al conectarse.
   - **Certificate Path** (Ruta de certificado): esta casilla está disponible si seleccionó la casilla de verificación Usa certificado. Seleccione **Pick** (Elegir) para buscar el archivo de certificado.
   - **Key Path** (Ruta de clave): esta casilla está disponible si seleccionó la casilla de verificación Usa certificado. Seleccione **Pick** (Elegir) para buscar la clave de red que le proporcionó su administrador.

Copyright © 2011, Juniper Networks, Inc.

5. Seleccione **Create Connection** (Crear conexión). Ahora se habrá creado y guardado su conexión.

Figura 35: Creación de una conexión

Conexión

Una vez que haya configurado su conexión, seleccione el botón **Connect** (Conectar) (consulte la Figura 32 en la página 34).

Si el campo **Select Connection** (Seleccionar conexión) no muestra la conexión predeterminada correcta, puede seleccionarla en el menú desplegable. Quizá deba ingresar información adicional que necesitará la red cuando establezca una conexión.

Visualización del estado de la conexión

El estado de su conexión actual se muestra también en la parte inferior de la ventana de Junos Pulse como un icono. La apariencia del icono indica si la conexión está activa o inactiva.

Conexión activa

Sin sesión

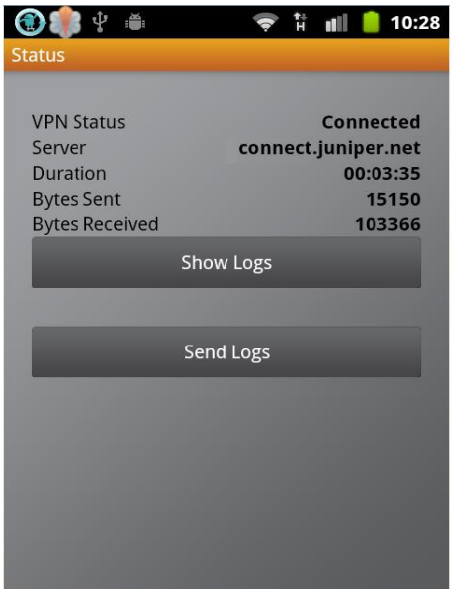
El icono de la conexión activa aparece también en la barra de estado de la parte superior de la pantalla del dispositivo. Al cerrar Junos Pulse, este icono permanece visible siempre que su conexión VPN esté activa.

Copyright © 2011, Juniper Networks, Inc.

Visualización de la pantalla de estado de la conexión

Cuando tiene una conexión VPN completa establecida (no todos los dispositivos admiten las funciones de VPN al completo), al seleccionar el botón **Status** (Estado) en la pantalla principal (consulte la Figura 32 en la página 34), se mostrará información sobre la VPN similar a la que se muestra en la Figura 36 en la página 37.

Figura 36: Pantalla de estado de la conexión VPN



En la barra de notificación, se mostrará también la notificación siguiente cuando tenga una conexión VPN activa. Consulte la Figura 37 en la página 37.

Figura 37: Notificación VPN

Utilización de las funciones de seguridad

El conjunto Junos Pulse Mobile Security ofrece acceso a funciones que protegen su dispositivo frente a malware y virus, y le permite respaldar la información del calendario y los contactos en un servidor central. Junos Pulse Mobile Security es una función opcional que habilita el administrador. Cuando está habilitada para su dispositivo, deberá registrar el dispositivo con Mobile Security Gateway antes de poder acceder al conjunto de funciones de seguridad.

Registro de seguridad

Su administrador puede configurar el registro de seguridad en el dispositivo para que se realice de forma automática, mediante URL o de forma manual.

Registro automático mediante URL

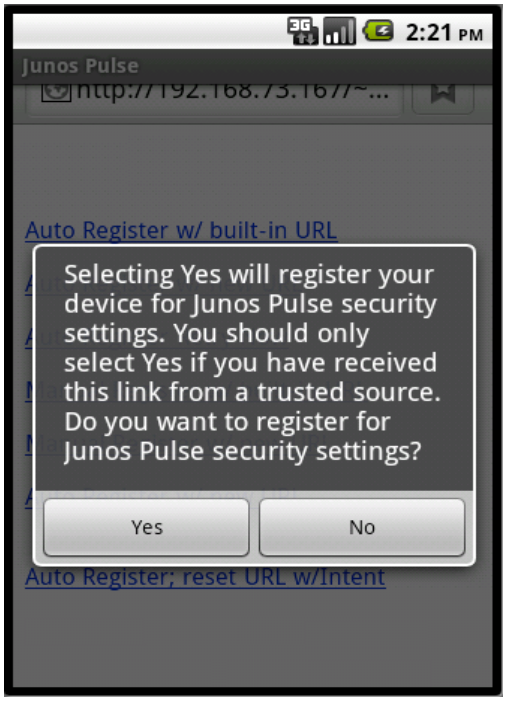
Para realizar el registro automático mediante URL, tendrá que seleccionar una URL proporcionada por su administrador. Cuando haga clic en la URL, se le mostrará un mensaje para que verifique que dicha URL proviene de una fuente confiable. Al hacer clic en **Yes** (Sí) tras recibir este mensaje, tendrá lugar el proceso de registro de seguridad automático.

Para registrar las funciones de seguridad de forma automática, haga lo siguiente:

1. Inicie Junos Pulse.
2. Seleccione la URL de registro que le ha proporcionado su administrador por correo electrónico, mensaje de texto o sitio Web.
3. Debido a que el registro automático modifica los ajustes de seguridad de su dispositivo, deberá verificar la validez de la URL. Si está seguro de que la URL es confiable, seleccione **Yes** (Sí) cuando se le solicite (consulte la Figura 38 en la página 38).

Después de haber seleccionado Sí, el dispositivo estará registrado automáticamente para las funciones de seguridad.

Figura 38: Solicitud de registro automático mediante URL


2:21 PM
Junos Pulse
Auto Register w/ built-in URL
Selecting Yes will register your device for Junos Pulse security settings. You should only select Yes if you have received this link from a trusted source. Do you want to register for Junos Pulse security settings?
Yes
No
Auto Register; reset URL w/Intent

Copyright © 2011, Juniper Networks, Inc.

Registro manual

En algunos casos, el registro manual también puede requerir que seleccione una URL proporcionada por su administrador. Cuando seleccione la URL, se le mostrará un mensaje para que verifique que dicha URL proviene de una fuente fiable (consulte la Figura 39 en la página 39). Al hacer clic en Yes (Sí) en la solicitud de registro, se mostrará la pantalla de registro manual.

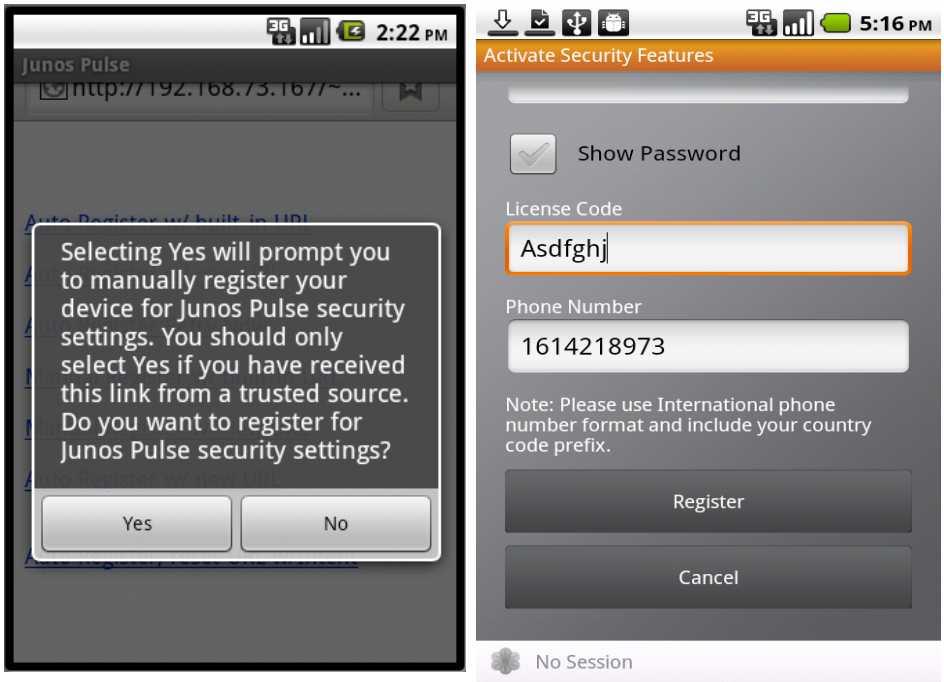
La pantalla de registro requiere que ingrese cierta información, como el código de licencia proporcionado por su administrador.

Nota informativa: si utiliza un dispositivo con WIFI solamente y no tiene acceso a una red celular, algunos campos (como el del número de teléfono) no se mostrarán.

Para registrar manualmente la seguridad, realice lo siguiente:

1. Inicie Junos Pulse.
1. Seleccione la **URL** que le ha proporcionado su administrador por correo electrónico, mensaje de texto o sitio Web.
2. Compruebe que la URL es confiable y haga clic en **Yes** (Sí) cuando se le solicite. Aparecerá la pantalla de registro (consulte la Figura 39 en la página 39).
3. Opcionalmente, ingrese una dirección de Correo electrónico y Contraseña. (La información de correo electrónico y de contraseña no se usa en este momento.)
4. Especifique el **código de licencia** que le proporcionó su administrador.
5. El número de teléfono del dispositivo aparece en el cuadro **Número de teléfono**. Si el número no aparece, ingréselo manualmente, incluidos el código de país y el código de área sin los prefijos internacionales '00' ni '+'. No utilice espacios, paréntesis ni caracteres especiales.
6. Seleccione **Register** (Registrar).

Figura 39: Solicitud de registro manual mediante URL y pantalla de registro

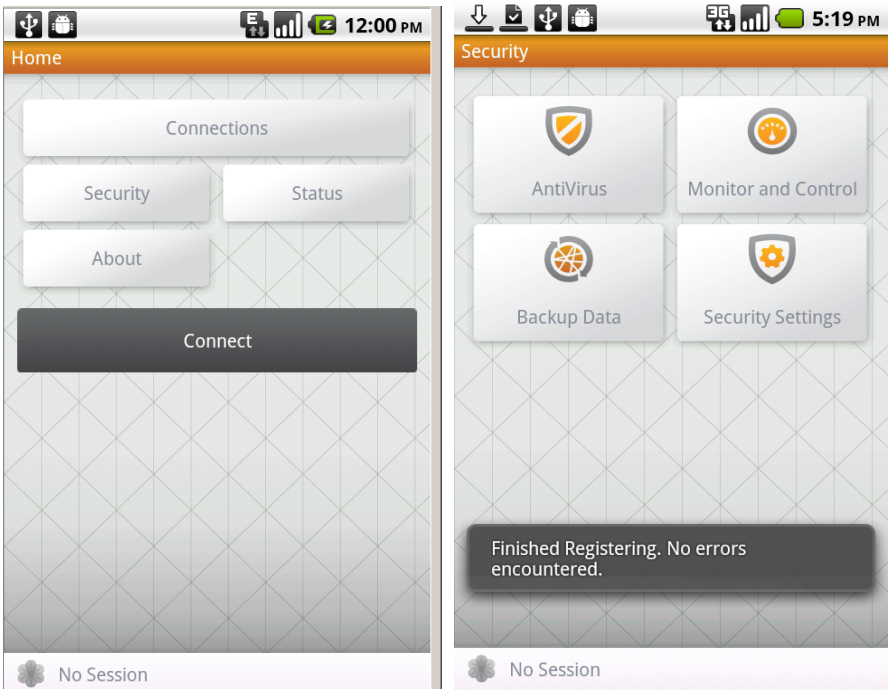

2:22 PM
Junos Pulse
Selecting Yes will prompt you to manually register your device for Junos Pulse security settings. You should only select Yes if you have received this link from a trusted source. Do you want to register for Junos Pulse security settings?
Yes
No
5:16 PM
Activate Security Features
Show Password
License Code
Asdfghj
Phone Number
1614218973
Note: Please use International phone number format and include your country code prefix.
Register
Cancel
No Session

Una vez que haya registrado las funciones de seguridad correctamente, se mostrarán las funciones disponibles, a las que podrá acceder con el botón de **seguridad** (consulte la Figura 40 en la página 40). Estas funciones son las siguientes:

- **AntiVirus and Malware Detection** (Antivirus y detección de malware): control de las actividades del antivirus y detección de malware instalado.
- **Monitor and Control** (Supervisión y control): visualización de los ajustes de supervisión.
- **Backup Data** (Respaldar datos): respaldo de la información del calendario y los contactos.
- **Security Settings** (Ajustes de seguridad): ajuste de los intervalos de los análisis de sistema.

Nota informativa: el administrador puede habilitar o deshabilitar las funciones de seguridad.

Figura 40: Funciones disponibles y funciones de seguridad



- **About** (Acerca de): ofrece información sobre la versión del software.

Antivirus

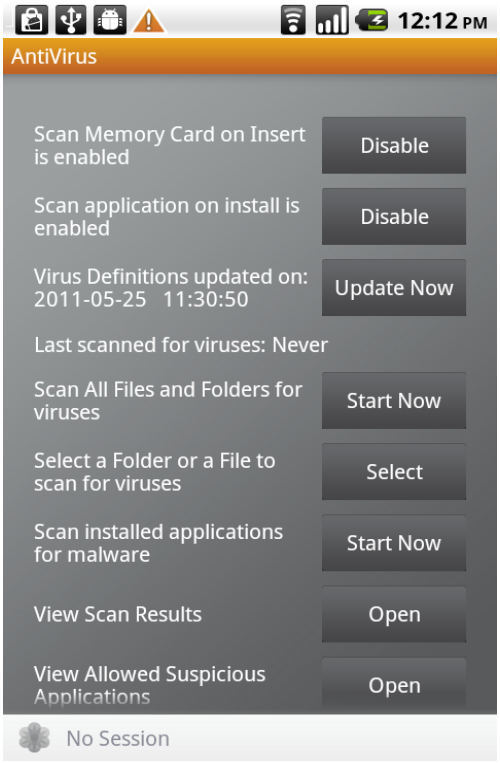
El servicio Antivirus protege su dispositivo al analizar todos los archivos y las tarjetas secure digital (SD) para prevenir la infección del dispositivo por parte de un malware que pueda estar almacenado en la tarjeta. Para configurar y ejecutar las funciones del antivirus:

1. Inicie Junos Pulse.
2. Seleccione **Security** (Seguridad).
3. Seleccione **Antivirus** y configure lo siguiente (consulte la Figura 41 en la página 41):
   - **Scan Memory Card on Insert** (Analizar tarjeta de memoria al insertarla): analiza la tarjeta de memoria en busca de malware y virus. Seleccione el botón disponible para **habilitar** esta función.
   - **Scan application on install** (Analizar la aplicación al instalarla): analiza las aplicaciones que intenta instalar en busca de malware. Seleccione el botón disponible para **habilitar** esta función.

Copyright © 2011, Juniper Networks, Inc.

- **Virus Definitions updated on** (Definiciones de virus actualizadas el): las definiciones más recientes se cargan al registrarse y se actualizan según la programación establecida por el administrador de seguridad. Seleccione **Update Now** (Actualizar ahora) para actualizar las definiciones manualmente.
- **Scan all files and folders for viruses** (Analizar todos los archivos y las carpetas en busca de virus): seleccione **Start Now** (Iniciar ahora) para iniciar un análisis completo de los datos del dispositivo.
- **Select a File or Folder to scan for viruses** (Seleccionar un archivo o carpeta en busca de virus): puede analizar un archivo o carpeta seleccionado, o la tarjeta SD instalada. Haga clic en **Select** (Seleccionar) para abrir la pantalla de sección de componentes y elija un objetivo para analizar.
- **Scan installed applications for malware** (Analizar aplicaciones instaladas en busca de malware): seleccione **Start Now** (Iniciar ahora) para analizar las aplicaciones en busca de malware.
- **View Scan Results** (Ver resultados del análisis): seleccione **Open** (Abrir) para ver los resultados de los análisis de virus y malware más recientes. Este botón le permite acceder a la pantalla de resultados del análisis que se describe en “Pantalla de resultados del análisis” en la página 42.
- **View Allowed Suspicious App** (Ver aplicaciones sospechosas permitidas): seleccione **Open** (Abrir) para ver la lista de las aplicaciones calificadas como sospechosas que ha permitido. En esta pantalla puede cambiar de opinión y no permitir la instalación de las aplicaciones de la lista. Para obtener más información, consulte página46.

Figura 41: Configuración del antivirus



Detección de malware, aplicaciones prohibidas y aplicaciones sospechosas

Junos Pulse detecta el malware de las aplicaciones por medio de listas negras que incluyen malware conocido y por medio de tecnología heurística para detectar aplicaciones que pueden ser sospechosas. Los análisis del dispositivo en busca de virus y malware se producen a intervalos regulares que determina su administrador.

Los análisis detectan también aplicaciones que no cumplen las normativas de la empresa. Éstas son aplicaciones que ha prohibido su administrador de red.

Pantalla de resultados del análisis

Si su administrador ha habilitado el antivirus en su dispositivo, la pantalla de resultados del análisis mostrará los virus, malware, aplicaciones sospechosas y aplicaciones prohibidas que tiene su dispositivo. Si su dispositivo no tiene el antivirus habilitado, sólo verá las aplicaciones prohibidas de su dispositivo.

Cada ficha disponible muestra los archivos o aplicaciones que entran dentro de la categoría de detección correspondiente. Puede acceder a la pantalla de resultados del análisis de una de las formas siguientes:

- En la pantalla de antivirus (consulte la Figura 41 en la página 41): haga clic en el botón **Open** (Abrir) de la opción Ver resultados del análisis.
- Con el icono de notificación: el icono de notificación aparece en la parte superior de la pantalla de Junos Pulse cuando existen virus o malware visibles en la pantalla de resultados del análisis. Seleccione la notificación cuando esté presente para abrir la pantalla de resultados del análisis.

- Con el análisis del dispositivo: cuando finaliza el análisis, si se encuentran virus o malware, aparecerá la pantalla de resultados del análisis.

Fichas con los resultados del análisis

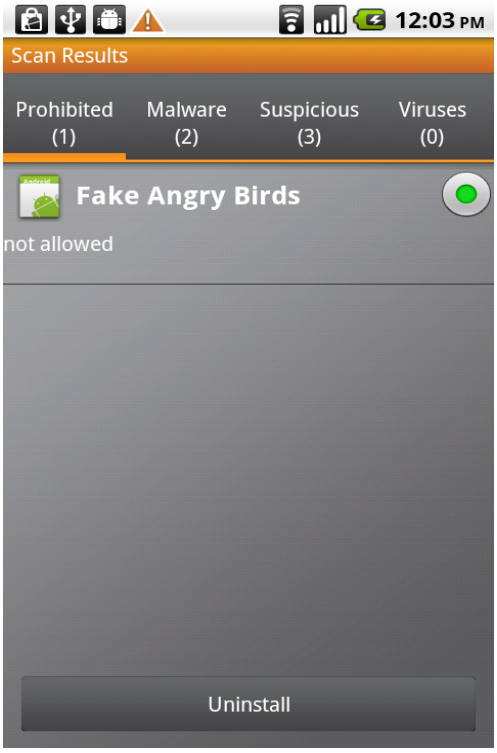
Un análisis puede detectar y calificar una aplicación de alguna de las formas siguientes en la pantalla de resultados del análisis:

Copyright © 2011, Juniper Networks, Inc.

- **Prohibida:** esta ficha (consulte la Figura 42 en la página 43) enumera las aplicaciones instaladas en el dispositivo que ha prohibido su administrador. Para eliminar una aplicación prohibida, seleccione el **radio button** (botón de opción) al lado del nombre de la aplicación y haga clic en el botón **Uninstall** (Desinstalar). Si no desinstala las aplicaciones que están prohibidas, el icono de notificación continuará apareciendo en la parte superior de la pantalla de Junos Pulse.

Nota informativa: en algunos dispositivos, Junos Pulse puede desinstalar automáticamente aplicaciones que están prohibidas.

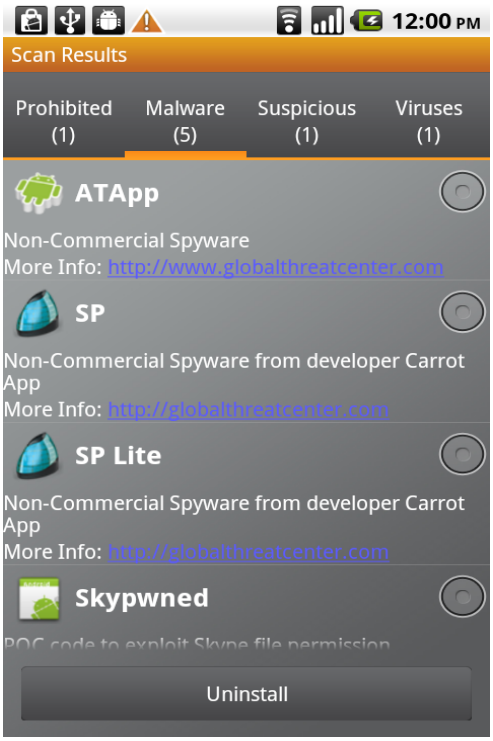
Figura 42: Ficha Prohibited (Prohibidas) de los resultados del análisis



- **Malware:** esta ficha (consulte la Figura 43 en la página 44) enumera las aplicaciones instaladas en el dispositivo que se sabe que contienen malware. Para eliminar el malware, seleccione el **radio button** (botón de opción) al lado del nombre de la aplicación y haga clic en el botón **Uninstall** (Desinstalar). Si no desinstala las aplicaciones que tienen malware, el icono de notificación continuará apareciendo en la parte superior de la pantalla de Junos Pulse.

Nota informativa: en algunos dispositivos, Junos Pulse puede desinstalar automáticamente aplicaciones que tienen malware.

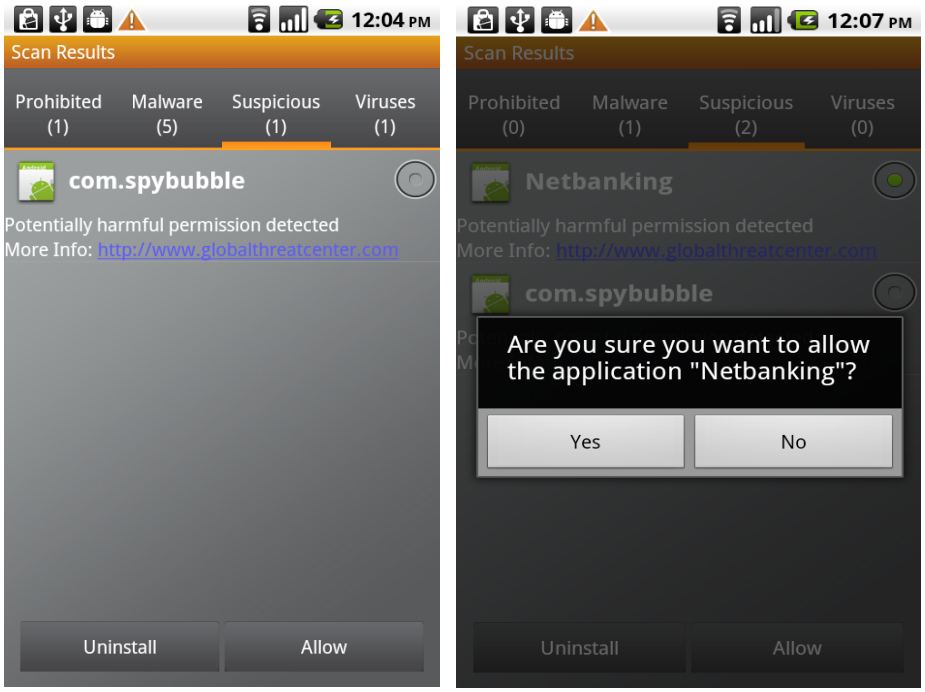
Figura 43: Ficha Malware de los resultados del análisis



Copyright © 2011, Juniper Networks, Inc.

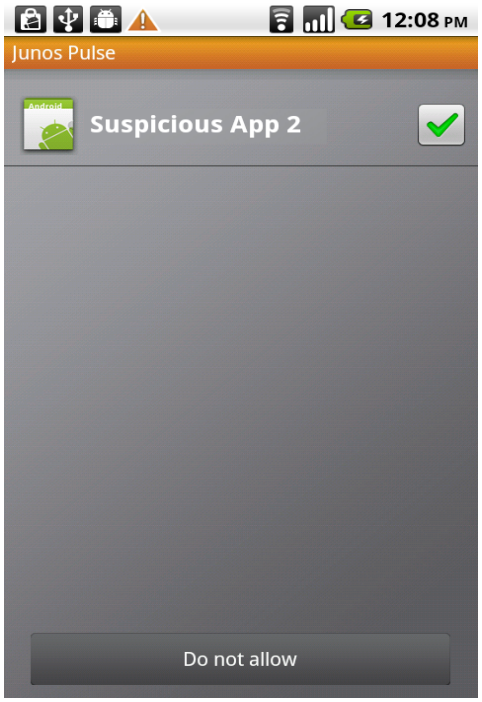
- **Sospechosas:** esta ficha (consulte la Figura 44 en la página 45) enumera las aplicaciones instaladas en el dispositivo que parecen sospechosas. Una aplicación se considera sospechosa cuando la tecnología heurística ha determinado que la aplicación puede ser malware. En el caso de las aplicaciones sospechosas, tiene la opción de permitir la aplicación o desinstalarla. Para permitir la aplicación sospechosa, seleccione el **radio button** (botón de opción) al lado del nombre de la aplicación y haga clic en el botón **Allow** (Permitir). También deberá hacer clic en **Yes** (Sí) para confirmar la acción Permitir. Para desinstalar una aplicación sospechosa, seleccione el **radio button** (botón de opción) al lado del nombre de la aplicación y haga clic en **Uninstall** (Desinstalar). Si no desinstala ni permite las aplicaciones sospechosas, el icono de notificación continuará apareciendo en la parte superior de la pantalla de Junos Pulse.

Figura 44: Ficha Suspicious (Sospechosas) de los resultados del análisis y solicitud de permiso



- **Aplicaciones sospechosas permitidas:** cuando permite una aplicación sospechosa, se le ofrecerá una pantalla independiente que le permitirá administrar las aplicaciones sospechosas en caso de que decida desinstalar una aplicación permitida después (consulte la Figura 45 en la página 46). Al seleccionar la **casilla de verificación** al lado del nombre de la aplicación y hacer clic en el botón **No permitir**, puede mover la aplicación permitida a la ficha **Suspicious** (Sospechosas). Puede acceder a la pantalla de aplicaciones permitidas desde la pantalla del antivirus, haciendo clic en el botón **Abrir de View Allowed Suspicious App** (Ver aplicaciones sospechosas permitidas). (Consulte la Figura 41 en la página 41).

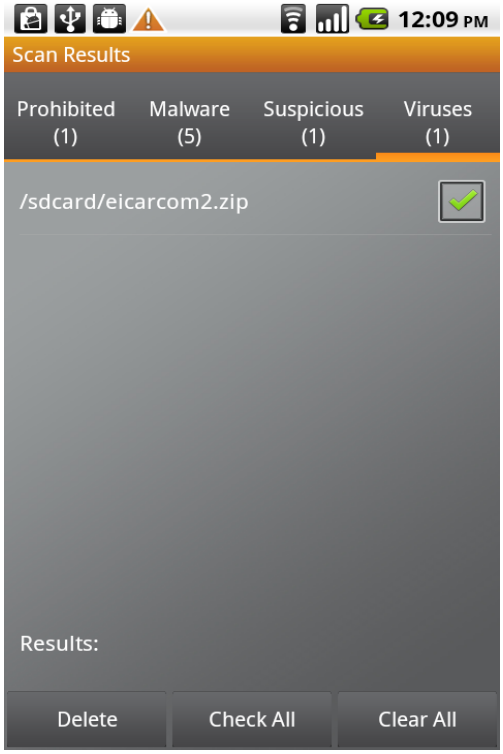
Figura 45: Pantalla de aplicaciones sospechosas permitidas



Copyright © 2011, Juniper Networks, Inc.

- **Virus:** esta ficha (consulte la Figura 46 en la página 47) enumera los virus encontrados en el último análisis. Se recomienda que elimine estos virus cuando se muestren aquí. Para eliminar los virus del dispositivo, seleccione **check box** (casilla de verificación) que se encuentra al lado del nombre del virus y haga clic en el botón **Delete** (Eliminar). Para eliminar varios virus a la vez, seleccione el botón **Check All** (Marcar todos) y, a continuación, el botón **Delete** (Eliminar).

Figura 46: Ficha Virus de los resultados del análisis



Supervisión y control

La pantalla Supervisión y control le permite ver los ajustes de Junos Pulse actuales además de los archivos de registro y eventos. Para utilizar la supervisión y control:

1. Inicie Junos Pulse.
2. Seleccione **Security** (Seguridad).
3. Seleccione **Monitor and Control** (Supervisión y control) (consulte la Figura 40 en la página 40).

La pantalla Supervisión y control muestra los ajustes que están vigentes actualmente junto con el límite de tamaño del archivo de registro y el límite de recuento de eventos. Si el volumen de datos excede los límites especificados, los datos en cuestión se cargan en el servidor.

Respaldo de datos

Junos Pulse Mobile Security respalda los contactos y la información de citas de calendario en una ubicación central.

Copyright © 2011, Juniper Networks, Inc.

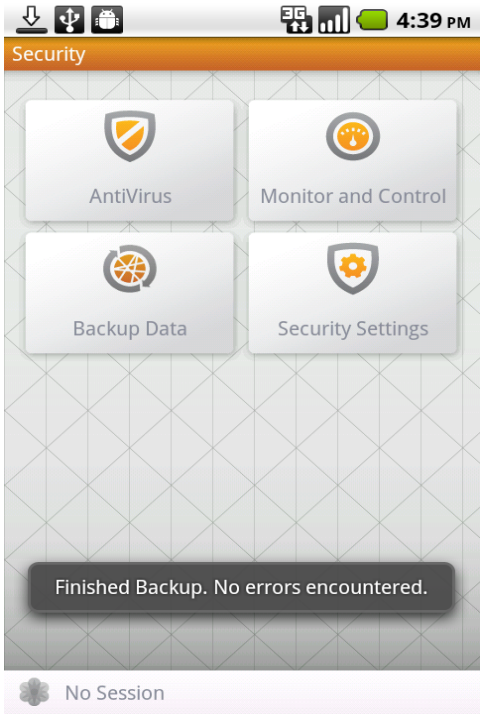
Para restaurar los datos, debe contactar al administrador. El administrador iniciará una restauración por medio de un comando SMS que le indica a su dispositivo que debe contactar con el servidor para recuperar el respaldo.

Para respaldar los datos del dispositivo:

1. Inicie Junos Pulse.
2. Seleccione **Security** (Seguridad).
3. Seleccione **Security Settings** (Respaldar datos) (consulte la Figura 40 en la página 40). Comenzará el respaldo de datos (consulte la Figura 47 en la página 48).

Para restaurar los datos del dispositivo, contacte con el administrador.

Figura 47: Respaldo de datos



Ajustes de seguridad

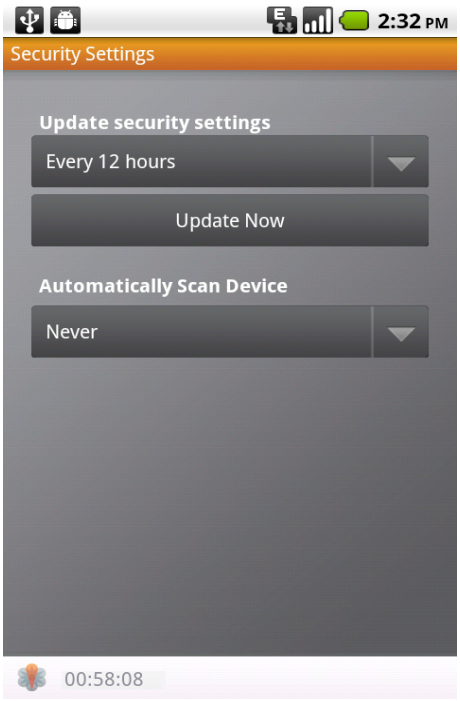
El administrador configura los ajustes de seguridad y los cambios se descargan al dispositivo. Puede modificar las actualizaciones de los ajustes de seguridad y los intervalos de análisis de la forma siguiente:

1. Inicie Junos Pulse.
2. Seleccione **Security** (Seguridad).
3. Seleccione **Security Settings** (Respaldar datos) (consulte la Figura 40 en la página 40).
4. O bien, realice lo siguiente (consulte la Figura 48 en la página 49).
   - **Update security settings** (Actualizar los ajustes de seguridad): puede especificar con qué frecuencia se comunicará el dispositivo con Junos Pulse para obtener los ajustes actualizados. Para realizar una actualización inmediata, haga clic en **Update Now** (Actualizar ahora).

Copyright © 2011, Juniper Networks, Inc.

- **Automatically scan device** (analizar el dispositivo automáticamente): normalmente, el administrador configura este ajuste y no se puede cambiar.

Figura 48: Ajustes de seguridad



Funciones antirrobo

Existen una serie de medidas que puede tomar para proteger el dispositivo en caso de pérdida o robo. Para activar las funciones antirrobo, póngase en contacto con el administrador. Estas funciones incluyen:

- **Lock Handset, Unlock Handset, Wipe Handset** (Bloquear el teléfono, desbloquear el teléfono, limpiar el teléfono): Estas funciones actúan de forma diferente en función de las versiones del sistema operativo Android:

  En Android 2.2 y superior

  - **Lock and Unlock Handset** (Bloquear y desbloquear el teléfono): si la función de administrador del dispositivo está activada, la única forma de desbloquear el dispositivo es enviar un comando de desbloqueo desde el servidor. Si la función de administrador del dispositivo no está activada, el dispositivo puede desbloquearse cuando se envíe un comando de desbloqueo desde el servidor o al ingresar la contraseña configurada durante el registro manual.
    - Botón de **llamada de emergencia:** cuando el dispositivo está bloqueado, existe un botón de llamada de emergencia disponible en la pantalla de desbloqueo. Esto le permite realizar una llamada a un número de emergencia, por ejemplo, cuando seleccione este botón y marque dicho número.
  - **Wipe Handset** (Limpiar el teléfono): si la función de administrador del dispositivo está activada, un comando de borrado que se envía desde el servidor restablecerá la configuración de fábrica en el teléfono. Si la función de administrador del teléfono no está activada, no se llevará a cabo la función de limpieza.

Copyright © 2011, Juniper Networks, Inc.

En Android 2.1

- **Lock and Unlock Handset** (Bloquear y desbloquear el teléfono): esta función bloquea el dispositivo hasta que se envíe un comando de desbloqueo desde el servidor o se ingrese la contraseña configurada durante el registro manual.
  - Botón de **llamada de emergencia:** cuando el dispositivo está bloqueado, existe un botón de llamada de emergencia disponible en la pantalla de desbloqueo. Esto le permite realizar una llamada a un número de emergencia, por ejemplo, cuando seleccione este botón y marque dicho número.
- **Wipe Handset** (Limpiar el teléfono): elimina la información de correo electrónico, programación, contactos y tareas.

- **Send Backup** (enviar respaldo): si estos datos no están almacenados en el servidor, esta función recopila la información de respaldo del dispositivo y la envía por correo electrónico a la dirección de correo electrónico proporcionada en el proceso de registro.
- **GPS Location** (Ubicación por GPS): si el dispositivo está equipado con GPS, el administrador podrá ubicarlo. La ubicación del dispositivo se muestra en el servidor de Junos Pulse.
- **Alarm On and Off** (Activación/desactivación de alarma): emite un sonido de alarma con un volumen máximo para ubicar el dispositivo cuando se encuentra en un lugar cercano.
- **GPS Theft On and Off** (Activación/desactivación de GPS por robo): envía actualizaciones del GPS al servidor de Junos Pulse cada 2 a 5 minutos para ajustar la ubicación por GPS en caso de robo del dispositivo.
- **SIM Change** (Cambio de SIM): incluye 2 ajustes:
  - Si se extrae la tarjeta SIM, el dispositivo activa el GPS por robo, el registro de Supervisión y control y bloquea el dispositivo.
  - Si la tarjeta SIM se cambia por otra, el dispositivo realiza todas las acciones anteriores y comprueba si está activado el indicador de borrado, con el fin de limpiar toda la información confidencial del dispositivo automáticamente.

Desinstalación o borrado de datos

Al registrar el dispositivo para obtener las funciones de seguridad, se está registrando con Mobile Security Gateway de Junos Pulse. En algunos casos, quizá deba registrar el dispositivo con un Mobile Security Gateway de Junos Pulse diferente después del registro inicial, o quizá deba borrar los ajustes de Junos Pulse del dispositivo por otro motivo. Puede conseguir esto desinstalando Junos Pulse o borrando manualmente todos los ajustes del siguiente modo.

1. Desde el menú principal, seleccione **Settings** (Ajustes) > **Applications** (Aplicaciones) > **Manage Applications** > (Administrar aplicaciones) > **Junos Pulse**.
2. Para desinstalar Junos Pulse, seleccione el botón **Uninstall** (Desinstalar) (consulte la Figura 49 en la página 51).

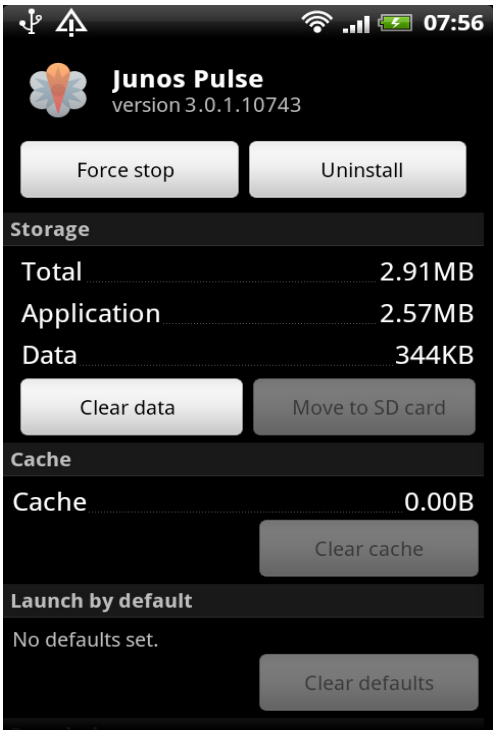
O bien:

3. Para borrar todos los datos de Junos Pulse, seleccione el botón **Clear data** (Borrar datos).

Su administrador le ofrecerá instrucciones para volver a registrar Junos Pulse.

Copyright © 2011, Juniper Networks, Inc.

Figura 49: Pantalla de información de la aplicación Junos Pulse



Funciones de seguridad de BlackBerry

Las secciones siguientes describen las funciones de Junos Pulse disponibles para la plataforma BlackBerry. Al hacer clic en el icono principal de **Junos Pulse** en la carpeta **Applications** (Aplicaciones), podrá acceder a las funciones de seguridad siguientes:

Antivirus

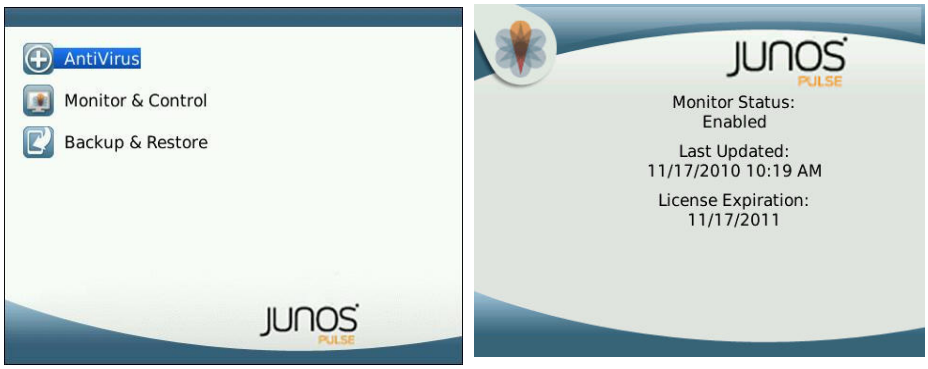
Seleccione la función de seguridad **Antivirus** para ver información sobre los controles del antivirus y sobre el archivo de registro. Al abrir Antivirus, verá la información siguiente: (consulte la Figura 50 en la página 52).

- Estado de supervisión: aquí podrá ver si la opción está habilitada o deshabilitada. Esta opción está habilitada de modo predeterminado.
- Última actualización: vea la fecha de la última actualización de las definiciones de virus.
- Fecha de vencimiento de licencia: vea la información de vencimiento de la licencia.

De manera predeterminada, la función de antivirus está configurada para analizar los archivos a medida que los recibe a través de algún mecanismo de transferencia de archivos (como correo electrónico, SMS/MMS o Bluetooth). También puede iniciar un análisis manual.

Copyright © 2011, Juniper Networks, Inc.

Figura 50: Información de visualización y de selección de antivirus de Junos Pulse en BlackBerry

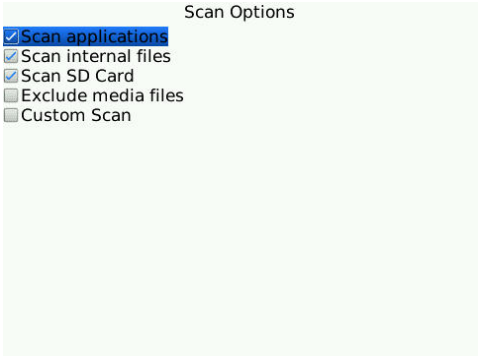


Análisis de virus manual

Al hacer clic en el botón **Menú** de su BlackBerry desde la ventana Antivirus, estará disponible la opción **Scan Now** (Analizar ahora).

1. Seleccione **Scan Now** (Analizar ahora) para realizar un análisis completo del dispositivo. Al seleccionar Analizar ahora, aparecerá la ventana **Scan Options** (Opciones de análisis). Consulte la Figura 51 en la página 52.

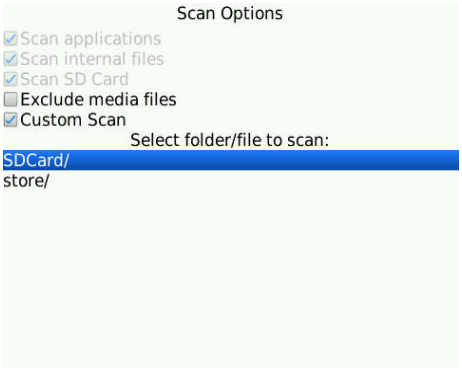
Figura 51: Scan Options (Opciones de análisis) de Junos Pulse en BlackBerry



2. En Scan Options (Opciones de análisis), están marcadas las tres primeras opciones de manera predeterminada para realizar un análisis completo. Estas son: **Scan applications** (Analizar aplicaciones), **Scan internal files** (Analizar archivos internos) y **Scan SD Card** (Analizar tarjeta SD). Seleccione el botón **Menú** y elija **Start scan** (Iniciar análisis) para analizar estos elementos.
3. También tiene la posibilidad de excluir los archivos multimedia del análisis. Para ello, seleccione la casilla de verificación **Exclude media files** (Excluir archivos multimedia).
4. O bien, realice un análisis personalizado en vez de realizar un análisis del dispositivo completo. Para ello, seleccione la casilla de verificación **Custom Scan** (Análisis personalizado). Al seleccionar Custom Scan (Análisis personalizado), podrá elegir qué archivos o carpetas desea analizar. Consulte la Figura 52 en la página 53.

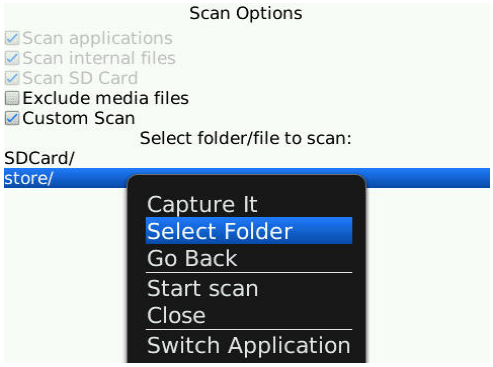
Copyright © 2011, Juniper Networks, Inc.

Figura 52: Selección de Custom Scan (Análisis personalizado) de Junos Pulse en BlackBerry



5. En Custom Scan (Análisis personalizado), resalte una carpeta disponible y haga clic en el botón **Menú** de su BlackBerry.
6. Seleccione **Select Folder** (Seleccionar carpeta) en el menú. Consulte la Figura 53 en la página 53. Para realizar un mayor desglose, repita estos pasos hasta que llegue al archivo o carpeta que desea analizar.

Figura 53: Selección de carpeta/archivo de análisis personalizado de Junos Pulse en BlackBerry



7. Haga clic en el botón **Menú** y seleccione **Start scan** (Iniciar análisis) para analizar los elementos seleccionados.

El progreso del análisis y los resultados del mismo se mostrarán cuando finalice el análisis.

Archivos en cuarentena

Durante el análisis, los archivos infectados encontrados se dejarán automáticamente en cuarentena. La cuarentena le permite decidir si eliminar o no los archivos infectados. Al hacer clic en el botón **Menú** de su BlackBerry desde la ventana **Antivirus Monitor Status** (Estado de supervisión del antivirus), estará disponible la lista **Quarantine** (Cuarentena).

Puede eliminar los archivos en cuarentena haciendo clic en el botón **Menú** y seleccionando **Delete** (Eliminar).

Copyright © 2011, Juniper Networks, Inc.

Análisis a demanda

Al hacer clic en el botón **Menú** de su BlackBerry desde la ventana **Antivirus Monitor Status** (Estado de supervisión del antivirus), estará disponible la opción **OnDemand Scan Log** (Registro de análisis a demanda). Este registro muestra información sobre los análisis que ha iniciado.

Registro de supervisión de archivos

Al hacer clic en el botón **Menú** de su BlackBerry desde la ventana **Antivirus Monitor Status** (Estado de supervisión del antivirus), estará disponible la opción **File Monitor Log** (Registro de supervisión de archivos). Este registro muestra marcas de hora asociadas a los cambios en los ajustes de supervisión de archivos.

Supervisión y control:

La pantalla Supervisión y control le permite ver los ajustes de Junos Pulse actuales además de los archivos de registro y eventos. Para utilizar la supervisión y control:

1. Inicie Junos Pulse.
2. Seleccione **Monitor and Control** (Supervisión y control) (consulte la Figura 50 en la página 52).

La pantalla Supervisión y control muestra los ajustes que están vigentes actualmente junto con el límite de tamaño del archivo de registro y el límite de recuento de eventos. Si el volumen de datos excede los límites especificados, los datos en cuestión se cargan en el servidor.

Respaldo & Restaurar

La función Respaldo & Restaurar le permite respaldar los contactos y los eventos del calendario almacenados en el dispositivo.

Para respaldar datos:

1. En la lista de funciones de Junos Pulse, seleccione **Backup & Restore** (Respaldo y restaurar). La pantalla Respaldo y restaurar muestra la fecha del último respaldo y la última restauración.
2. En la ventana **Backup & Restore** (Respaldo y restaurar), haga clic en el botón **Menú**.
3. Seleccione **Backup Data** (Respaldar datos) desde el menú. Consulte la Figura 54 en la página 54. Esta información se enviará al servidor central.

Figura 54: Respaldo de datos de Junos Pulse en el dispositivo BlackBerry

Copyright © 2011, Juniper Networks, Inc.

4. Cuando ha finalizado el respaldo, haga clic en **OK** (Aceptar) en la ventana **Backup Successful** (Copia de seguridad correcta) que se muestra.

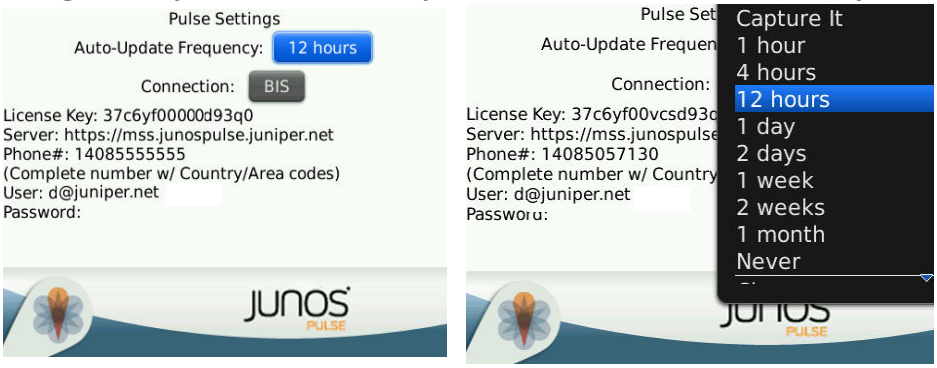
Sólo podrá iniciar una restauración desde el panel. Al iniciar una restauración, un comando SMS indica al dispositivo que contacte con el servidor para recuperar los datos respaldados. Consulte la “Comandos” en la página 22.

Ajustes

En la lista de funciones principal de Junos Pulse, haga clic en el botón de menú de su BlackBerry para acceder a los ajustes de actualización de seguridad y a la información general.

1. Al hacer clic en el botón de **menú** de su BlackBerry desde la ventana de funciones principal de Junos Pulse, estará disponible la opción **Settings** (Ajustes).
2. Seleccione **Settings** (Ajustes). Se abrirá la ventana Ajustes de Pulse.
3. En la ventana Ajustes, se mostrará el ajuste **Auto-Update Frequency** (Frecuencia de actualización automática). De manera predeterminada, ésta está establecida en 12 horas. Puede cambiar este ajuste de 1 hora a 1 mes o a nunca seleccionándolo y desplazándose hasta la frecuencia que desee.

Figura 55: Ajustes de actualización y frecuencia de Junos Pulse en BlackBerry



4. En la ventana Ajustes, estará disponible el tipo de **conexión**. Si el dispositivo lo administra un servidor de administración de BlackBerry corporativo, su administrador le indicará qué método debe utilizar (BIZ o BEZ) para la conexión del dispositivo. De lo contrario, puede utilizar los ajustes de conexión estándar APN.

Funciones antirrobo

Las protecciones antirrobo para el dispositivo se configuran desde el panel.

Las funciones antirrobo incluyen:

- **Lock and Unlock Handset** (Bloquear y desbloquear teléfono): si el dispositivo está bloqueado, puede desbloquearse cuando se envíe un comando de desbloqueo desde el servidor o cuando se ingresa la contraseña configurada durante el registro manual.
  - Botón de **llamada de emergencia:** cuando el dispositivo está bloqueado, existe un botón de llamada de emergencia disponible en la pantalla de desbloqueo. Esto le permite realizar una llamada a un número de emergencia, por ejemplo, cuando seleccione este botón y marque dicho número.

Copyright © 2011, Juniper Networks, Inc.

- **Wipe Handset** (Limpiar teléfono): el comando de borrado enviado desde el servidor elimina los contactos, eventos, tareas y mensajes de correo electrónico. Los mensajes de texto no se eliminan. Si la cuenta de correo electrónico del dispositivo se establece para que se sincronice con el servidor (la opción predeterminada), la eliminación con la sincronización puede eliminar también los mensajes de correo electrónico del servidor.
- **Send Backup** (Enviar respaldo): si estos datos no están almacenados en el servidor, esta función recopila la información de respaldo del dispositivo y la envía por correo electrónico a la dirección de correo electrónico proporcionada en el proceso de registro.
- **GPS Location** (Ubicación por GPS): si el dispositivo está equipado con GPS, el administrador podrá ubicarlo. La ubicación del dispositivo se muestra en el servidor de Junos Pulse.
- **Alarm On and Off** (Activación/desactivación de alarma): emite un sonido de alarma con un volumen máximo para ubicar el dispositivo cuando se encuentra en un lugar cercano.
- **GPS Theft On and Off** (Activación/desactivación de GPS por robo): envía actualizaciones del GPS al servidor de Junos Pulse cada 2 a 5 minutos para ajustar la ubicación por GPS en caso de robo del dispositivo.
- **SIM Change** (Cambio de SIM): incluye 2 ajustes:
  - Si se extrae el SIM, el dispositivo activa el GPS por robo, el registro de Supervisión y control y bloquea el dispositivo.
  - Si el SIM se cambia por otro, el dispositivo realiza todas las acciones anteriores y comprueba si está activado el indicador de borrado, con el fin de limpiar toda la información confidencial del dispositivo automáticamente.

Funciones de seguridad iOS

Junos Pulse le permite acceder a los recursos de red protegidos desde su dispositivo Apple iOS™ a través de una conexión VPN segura. El componente de seguridad, el conjunto Junos Pulse Mobile Security, incluye las herramientas siguientes para reducir los riesgos de pérdida o robo del dispositivo:

- **Lock Device** (Bloquear dispositivo): bloquea el dispositivo en caso de pérdida o robo, o en caso de que desee que el dispositivo deje de funcionar por algún otro motivo.
- **Unlock Device** (Desbloquear dispositivo): desbloquea el dispositivo.
- **Retrieve App List** (Recuperar lista de aplicaciones): actualiza la lista de aplicaciones instaladas en el dispositivo.
- **Wipe Device** (Limpiar dispositivo): elimina los datos personales del dispositivo, como contactos, eventos del calendario, notas, historial de llamadas, carpetas de mensajes, y todos los datos de la tarjeta SD.

Copyright © 2011, Juniper Networks, Inc.

Conexión con Junos Pulse

Además de las funciones de seguridad descritas anteriormente, puede utilizar Junos Pulse para establecer una conexión VPN segura con su red corporativa utilizando la conectividad 3G, 4G, Edge o WIFI del dispositivo. Una vez que se ha establecido una conexión VPN, Junos Pulse puede incluir las funciones siguientes (consulte la Figura 32 en la página 34).

- **Intranet:** inicia las conexiones con el sitio interno configurado por el administrador.
- **Correo electrónico:** inicia la aplicación de correo electrónico.
- **Estado:** le permite ver, eliminar y enviar por correo electrónico los archivos de registro, lo que puede ser necesario para operaciones de solución de problemas. Los archivos de registro le muestran todos los incidentes de seguridad, como las horas de análisis para detección de virus y los virus descubiertos. Si cuenta con una conexión VPN establecida, también podrá ver el estado de dicha conexión en esta pantalla.
- **Acerca de:** ofrece información sobre la versión del software.

Nota informativa: Las pantallas de los iOS diferentes pueden variar.

Figura 56: Funciones disponibles como se muestran para iPhone

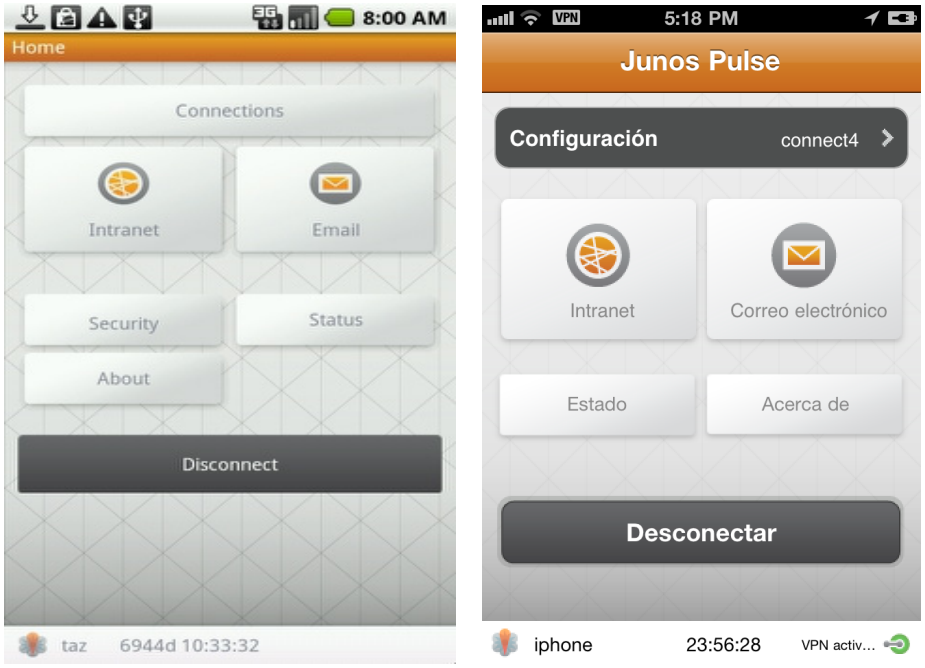
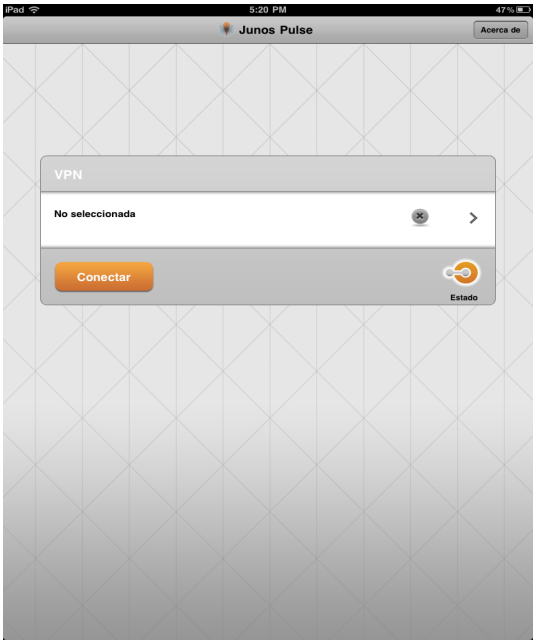


Figura 57: Funciones disponibles como se muestran para iPad



Adición de un perfil de conexión segura

Puede agregar una conexión VPN para cada red diferente a la que se conecte. Para definir un perfil de conexión, realice lo siguiente:

1. Inicie Junos Pulse.
2. Haga clic en **Configuration** (Configuración).
3. Si ya tiene un perfil de conexión configurado y está agregando un perfil adicional, haga clic en **Edit** (Editar).
4. Haga clic en **Add New Connection** (Agregar nueva conexión). Se abrirá la ventana Agregar. Consulte la Figura 58 en la página 59.

Nota informativa: las pantallas de los iOS diferentes pueden variar.

Copyright © 2011, Juniper Networks, Inc.

Figura 58: Adición de conexión en iPhone

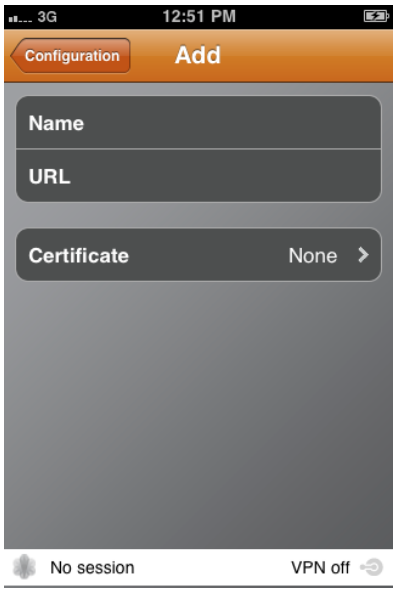
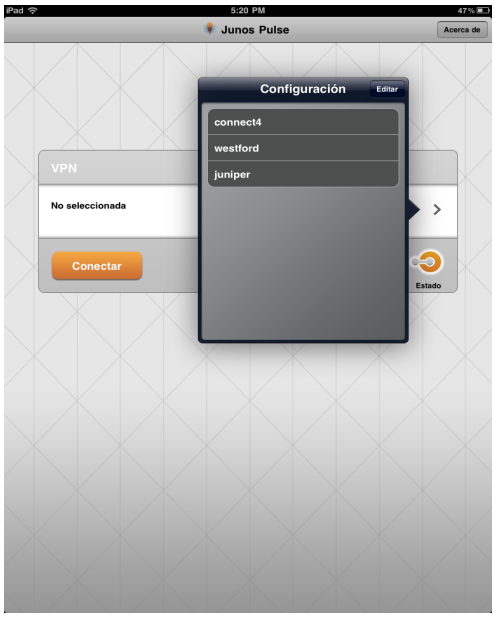


Figura 59: Adición de configuración en iPad



5. Especifique las propiedades del perfil de conexión.
   - **Nombre:** el nombre o descripción para este perfil de conexión.
   - **URL:** la dirección Web proporcionada por el administrador de red.
   - **Certificado:** si el administrador de red le proporcionó un certificado digital (normalmente por medio de un mensaje de correo electrónico o como archivo adjunto a un mensaje), haga clic en Certificate (Certificado). Cuando se abra la pantalla Identidades, seleccione el certificado que desea usar con este perfil. Si no usa un certificado, debe proporcionar un nombre de usuario y contraseña cuando utilice este perfil de conexión.
6. Haga clic en **Configuration** (Configuración) para volver a la ventana principal de Junos Pulse.

Conexión

Una vez que haya configurado su conexión, realice lo siguiente para conectarse.

1. Inicie Junos Pulse.
2. Haga clic en **Connect** (Conectar).
3. Cuando se abra la ventana Conectar, ingrese su **nombre de usuario** y **contraseña** de inicio de sesión. Consulte la Figura 60 en la página 60.
4. Haga clic en **Sign In** (Iniciar sesión).

Figura 60: Conectar

Visualización del estado de la conexión

El estado de su conexión actual se muestra también en la parte inferior de la ventana de Junos Pulse como un icono. La apariencia del icono indica si la conexión está activa o inactiva. Consulte también la Figura 32 en la página 34.

Conexión activa Sin sesión

Copyright © 2011, Juniper Networks, Inc.

Funciones de seguridad de Windows Mobile

Al hacer clic en el icono de Junos Pulse en la carpeta Programs (Programas), podrá acceder a las funciones siguientes:

Estado

Seleccione **Status** (Estado) para ver y enviar los archivos de registro. Consulte la Figura 61 en la página 62.

- En la ventana **Status** (Estado), haga clic en **Show Logs** (Mostrar registros) para ver los registros de análisis del antivirus. Haga clic en **Clear Logs** (Borrar registros) para eliminar los registros del análisis.
- En la ventana **Status** (Estado), haga clic en **Send Logs** (Enviar registros) para enviar los registros de análisis del antivirus por correo electrónico o SMS.

Conexión

Junos Pulse usa la conectividad 3G, 4G, Edge o WIFI de su dispositivo para establecer una conexión autenticada con una red protegida. Puede agregar una conexión para cada red diferente a la que se conecte. Consulte la Figura 61 en la página 62. Para definir una conexión:

1. Seleccione **Connections** (Conexiones).
2. Seleccione **Add Connection** (Agregar conexión) y especifique las propiedades de conexión.
   - **Nombre de la conexión:** un nombre descriptivo.
   - **URL:** la dirección Web proporcionada por el administrador de red.
3. Seleccione **Save** (Guardar).

El estado de su conexión actual aparece en la parte inferior de la ventana en la barra de estado.

Conectar

Para conectarse a una conexión que ya se ha configurado, realice lo siguiente:

1. Seleccione **Connect** (Conectar).
2. Ingrese su **nombre de usuario** y **contraseña**.
3. Haga clic en **Sign In** (Iniciar sesión).

Cuando su nombre de usuario y contraseña hayan sido aceptados, podrá acceder a las funciones de Junos Pulse proporcionadas a través de su conexión corporativa.

Correo electrónico e Intranet

Una vez que ha establecido una conexión a una red protegida, tendrá a su disposición las funciones de correo electrónico e Intranet. Puede acceder a los ajustes de correo electrónico e Intranet configurados por el administrador de la red protegida a la que se ha conectado a través de los botones de Intranet y Correo electrónico. Consulte la Figura 61 en la página 62.

Copyright © 2011, Juniper Networks, Inc.

Figura 61: Ventana principal de Junos Pulse en Windows Mobile

Utilización de las funciones de seguridad

Seleccione el icono de **Junos Pulse** de la carpeta **Programs** (Programas) para acceder a las funciones de Pulse disponibles para su dispositivo. Seleccione **Security (**Seguridad) para ver y editar las funciones siguientes. Consulte la Figura 62 en la página 62.

Figura 62: Funciones de seguridad de Junos Pulse en Windows Mobile

Copyright © 2011, Juniper Networks, Inc.

Ajustes de seguridad

Haga clic en **Security Settings** (Ajustes de seguridad) para actualizar todos los ajustes de seguridad para el dispositivo y para actualizar la ubicación del dispositivo. Haga clic en **Save** (Guardar) si realiza algún cambio en estos ajustes. Consulte la Figura 63 en la página 63. Están disponibles los ajustes de seguridad siguientes.

- **Update security settings and data** (Actualizar ajustes de seguridad y datos): seleccione un margen de tiempo para recibir las actualizaciones de los ajustes de seguridad. Además de las definiciones de virus, los ajustes de seguridad incluyen los cambios que haya realizado en el dispositivo desde el panel. (Los ajustes de seguridad no incluyen los comandos que pueda enviar desde la ficha Inicio. Estos comandos se envían inmediatamente.) En la lista desplegable disponible, puede seleccionar: Nunca, Cada hora, Cada 4 horas, Cada 12 horas, Cada día, Cada 2 días, Cada semana, Cada 2 semanas y Cada mes.
- **Update** (Actualizar): haga clic en el botón **Update** (Actualizar) para realizar inmediatamente una actualización manual de los ajustes de seguridad.
- **Device Location** (Ubicación del dispositivo): seleccione un margen de tiempo para recibir información automática sobre la ubicación del dispositivo: Nunca, Cada hora, Cada 4 horas, Cada 12 horas, Cada día, Cada 2 días, Cada semana, Cada 2 semanas y Cada mes.

Figura 63: Ajustes de seguridad de Junos Pulse en Windows Mobile

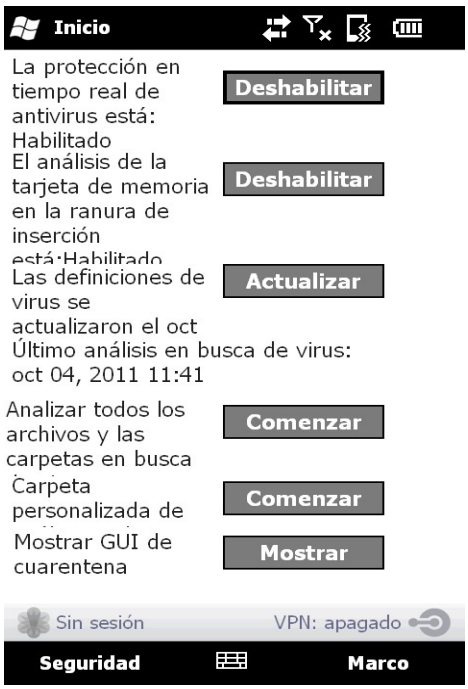
Antivirus

Seleccione la función de seguridad **Antivirus** para ver información sobre los controles del antivirus y sobre el archivo de registro. Cuando abra Antivirus, verá controles que le permitirán realizar un análisis de virus en la tarjeta de memoria, en el dispositivo completo o sólo en archivos y carpetas, así como actualizar las firmas de virus. Los controles de antivirus disponibles son los siguientes.

Copyright © 2011, Juniper Networks, Inc.

- **Antivirus Scanning** (Análisis de antivirus): el análisis del antivirus puede estar **habilitado** o **deshabilitado**.
- **Scan Memory Card on Insert** (Analizar tarjeta de memoria al insertarla): esta función está **habilitada** o **deshabilitada**.
- **Virus Definitions updated** (Definiciones de virus actualizadas): este campo indica la hora y fecha de la última actualización. Haga clic en el botón **Update Now** (Actualizar ahora) para realizar una actualización manual de las definiciones de virus.
- **Scan all files and folders for viruses** (Analizar todos los archivos y las carpetas en busca de virus): este campo indica la hora y fecha del último análisis. Haga clic en el botón **Start Now** (Iniciar ahora) para realizar un análisis manual de virus en todo el dispositivo. Un análisis completo puede tardar varios minutos en realizarse.
- **Scan custom folder for viruses** (Analizar la carpeta personalizada en busca de virus): le permite analizar un archivo o carpeta seleccionado o la tarjeta SD instalada. Haga clic en **Start Now** (Iniciar ahora) para abrir la pantalla de componentes y elija un objetivo para analizar.
- **Show Quarantine GUI** (Mostrar GUI de cuarentena): seleccione **Show** (Mostrar) para ver los archivos que hayan sido puestos en cuarentena por el análisis del antivirus.

Figura 64: Ajustes de antivirus de Junos Pulse en Windows Mobile



Antispam

El servicio antispam protege su dispositivo frente a llamadas no solicitadas y spam de SMS. El menú antispam le proporciona opciones para crear, personalizar y eliminar listas negras que se usen para filtrar spam. Para configurar y ejecutar las funciones del antispam:

1. Seleccione **Antispam** y configure lo siguiente (consulte la Figura 65 en la página 65):
   - **Nombre:** ingrese el nombre de la persona cuyas llamadas o mensajes desea bloquear.

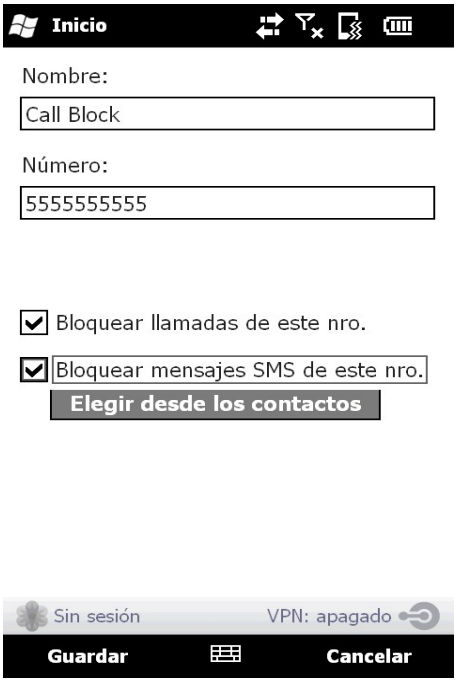
Copyright © 2011, Juniper Networks, Inc.

- **Número:** ingrese el número cuyas llamadas o mensajes desea bloquear.
- **Block Calls from this number** (Bloquear las llamadas desde este número): seleccione esta casilla de verificación para bloquear las llamadas de voz que se originen en el número que ingresó.
- **Block SMS messages from this number** (Bloquear los mensajes desde este número): seleccione esta casilla de verificación para bloquear los mensajes SMS que se originen en el número que ingresó.

2. Seleccione **Choose from Contacts** (Elegir desde contactos) si desea usar un número de su lista de contacto.
3. Seleccione **Save** (Guardar).

Nota informativa: haga clic en **Add** (Agregar) en la ventana Antispam para agregar números adicionales que desee bloquear.

Figura 65: Ajustes de antispam de Junos Pulse en Windows Mobile



Cuando haya ingresado al menos un número a la función antispam, la ventana Antispam cambia para permitir agregar números adicionales. También puede seleccionar **Enable Shortcode Blocking** (Permitir el bloqueo de código breve) en la ventana Antispam después de tener al menos una entrada. Consulte la Figura 66 en la página 66.

El bloqueo de código breve no es específico a ninguna de las entradas que agregó. Bloquea todas las llamadas de códigos breves. Los códigos breves son números telefónicos especiales que son significativamente más cortos, con cinco o menos dígitos. Los códigos breves se usan frecuentemente para marketing o promociones, y por lo tanto puede desear bloquearlos.

Copyright © 2011, Juniper Networks, Inc.

Figura 66: Bloqueo de código breve antispam de Junos Pulse en Windows Mobile

Nota informativa: deberá tener al menos un número configurado de bloqueo para ver las funciones que se muestran en la ventana Antispam de la Figura 66 en la página 66.

Cortafuegos

Las funciones de seguridad del cortafuegos le permiten bloquear o permitir el tráfico de datos hacia o desde el dispositivo usando listas de reglas que controlan el tráfico en base al número de puerto, dirección IP y otras opciones. Para configurar las funciones del cortafuegos, realice lo siguiente:

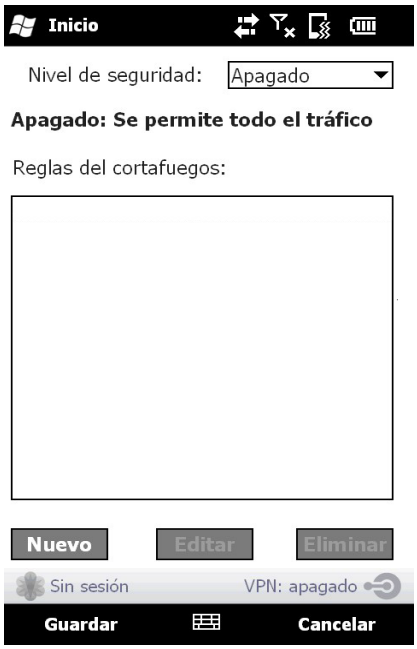
1. Seleccione Firewall (Cortafuegos) y configure lo siguiente (consulte la Figura 67 en la página 67):

   Security Level (Nivel de seguridad): seleccione un nivel de seguridad en la lista desplegable. Cuando seleccione un nivel, se agregan reglas de cortafuegos correspondientes a ese nivel a su lista de reglas activas. Puede establecer el nivel de seguridad de la forma siguiente.

   - **Low** (Bajo): para bloquear elementos concretos.
   - **High** (Alto): para permitir el tráfico de datos en los puertos y direcciones permitidos únicamente.
   - **Off** (Desactivado): para anular la protección del cortafuegos.

Copyright © 2011, Juniper Networks, Inc.

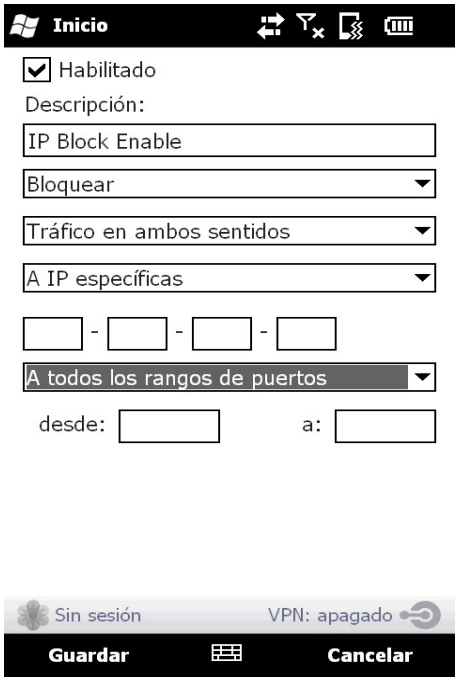
Figura 67: Ventana principal del cortafuegos de Junos Pulse en Windows Mobile



2. Haga clic en el botón **New** (Nuevo) para agregar una nueva regla a la lista de reglas activas del cortafuegos. Consulte la Figura 68 en la página 68. Puede configurar reglas para agregar entradas que se bloquearán o permitirán.
3. Para crear una regla de cortafuegos nueva, configure lo siguiente:
   - Seleccione la casilla de verificación para **habilitar** la regla. Puede crear una regla y dejarla deshabilitada con la posibilidad de utilizarla después.
   - Ingrese una **descripción** de la regla.
   - Seleccione **Block** (Bloquear) o **Allow** (Permitir) en la lista desplegable.
   - Seleccione **Inbound Traffic** (Tráfico entrante) o **Outbound Traffic** (Tráfico saliente) en la lista desplegable.
   - Puede crear esta regla para permitir/bloquear **todas las direcciones IP**, **direcciones IP específicas** o un **rango de direcciones IP**.
   - Si selecciona Specific IP addresses (IP específicas) o Range of IPs (Rango de direcciones IP), ingrese esa información en los campos de direcciones IP proporcionados. (Tenga en cuenta que puede utilizar una entrada comodín (*) para indicar el bloqueo de todo lo que se encuentre dentro del octeto en cuestión).
   - Puede crear esta regla para permitir/bloquear direcciones de puertos. Seleccione **To a Range of Ports** (A un rango de puertos) e ingrese esa información de puertos en los campos **desde** y **a** proporcionados o seleccione **All Ports** (A todos los puertos).
4. Haga clic en **Save** (Guardar).

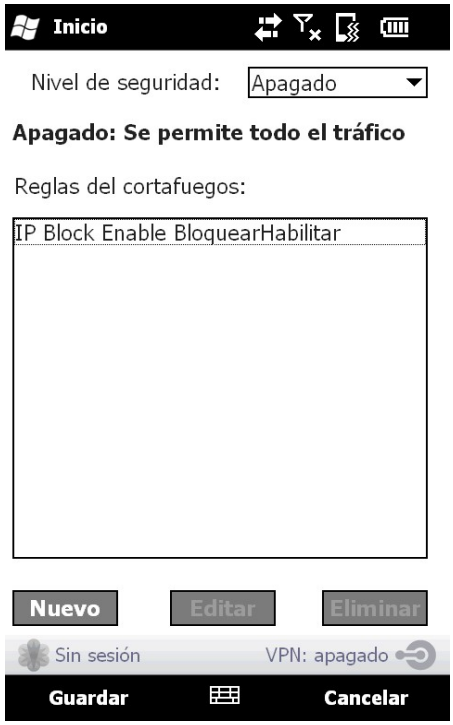
Copyright © 2011, Juniper Networks, Inc.

Figura 68: Ventana de reglas del cortafuegos de Junos Pulse en Windows Mobile



Cuando guarde una regla, se mostrará en la lista de reglas. Consulte la Figura 69 en la página 68.

Figura 69: Ventana de lista de reglas del cortafuegos de Junos Pulse en Windows Mobile



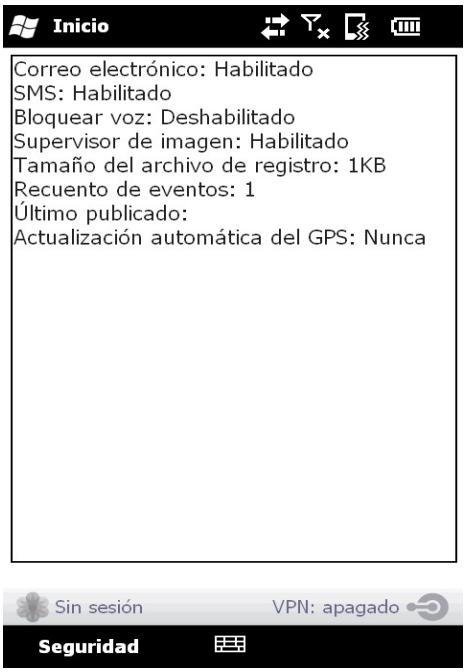
Copyright © 2011, Juniper Networks, Inc.

Nota informativa: seleccione una regla en la lista de reglas y utilice los botones **Edit** (Editar) y **Delete** (Eliminar) para realizar cambios en la regla existente y para eliminar reglas de la lista de reglas.

Supervisión y control

Seleccione **Monitor and Control** (Supervisión y control) para ver los ajustes del dispositivo que se han habilitado desde el panel. Por ejemplo, puede ver una lista de funciones de control, seguridad o antirrobo con la palabra "habilitada" o "deshabilitada" junto a ellas. El período de actualización de GPS y los límites de registro también pueden verse en esta ventana. Consulte la Figura 70 en la página 69.

Figura 70: Monitorización y control de Junos Pulse en Windows Mobile



Respaldo de datos

Puede respaldar la información de citas del calendario y los contactos en el panel desde el dispositivo con Windows Mobile.

Para respaldar los datos del dispositivo, realice lo siguiente.

1. Seleccione **Backup Data** (Respaldar datos).
2. En la ventana Respaldar datos, haga clic en **Backup Contacts and Calendar** (Respaldar contactos y calendario). Se le pedirá entonces que confirme que desea iniciar el respaldo. Haga clic en **Yes** (Sí). Comienza el respaldo. Cuando el respaldo finalice, verá una notificación en el dispositivo. Consulte la Figura 71 en la página 70.

Copyright © 2011, Juniper Networks, Inc.

Figura 71: Respaldo de datos y confirmación de Junos Pulse en Windows Mobile

Inicio
El respaldo de sus contactos y calendario los almacenará en el servidor para que se puedan restablecer al dispositivo más tarde.
Respaldar contactos y calendario
Inicio
El respaldo de sus contactos y calendario los almacenará en el servidor para que se
¿Confirma la operación de respaldo?
Sus contactos y el calendario se respaldarán y cargarán. ¿Desea continuar?
Yes
No
Sin sesión
VPN: apagado
Seguridad
Marco
Sin sesión
VPN: apagado
Seguridad
Marco

Sólo podrá iniciar una restauración desde el dispositivo. Al iniciar una restauración, un comando SMS indica al dispositivo que contacte con el servidor para recuperar los datos respaldados. Consulte “Comandos” en la página 22.

Funciones antirrobo

Las protecciones antirrobo para el dispositivo se configuran desde el dispositivo.

Las funciones antirrobo incluyen:

- **Lock Handset** (Bloquear el teléfono): bloquea el teléfono hasta que se envíe el comando de desbloqueo. Si el dispositivo está protegido con contraseña, continuará bloqueado incluso si se ingresa la contraseña correcta.
- **Unlock Handset** (Desbloquear teléfono): desbloquea el dispositivo.
- **Wipe Handset** (Desbloquear teléfono): elimina la información de correo electrónico, programación, contactos y tareas.
- **Send Backup** (Enviar respaldo): si estos datos no están almacenados en el servidor, esta función recopila la información de respaldo y la envía por correo electrónico a la dirección de correo electrónico proporcionada en el proceso de registro.
- **GPS Location** (Ubicación por GPS): si su BlackBerry tiene GPS, puede ubicar su dispositivo. La ubicación del dispositivo se muestra en un mapa en la pestaña Inicio.
- **Alarm On and Off** (Activación/desactivación de alarma): emite un sonido de alarma con un volumen máximo para ubicar el dispositivo cuando se encuentra en un lugar cercano.
- **GPS Theft On and Off** (Activación/desactivación de GPS por robo): envía actualizaciones del GPS al servidor cada 2 o 5 minutos para ajustar la ubicación por GPS en caso de robo del dispositivo.
- **SIM Change** (Cambio de SIM): incluye 2 ajustes:

Copyright © 2011, Juniper Networks, Inc.

- Si se extrae la tarjeta SIM, el dispositivo activa el GPS por robo, el registro de supervisión y control y bloquea el dispositivo. Puede desbloquear el teléfono con un nombre de usuario y contraseña.
- Si la tarjeta SIM se cambia por otra, el dispositivo realiza todas las acciones anteriores y comprueba si está activado el indicador de borrado, con el fin de limpiar toda la información confidencial del dispositivo automáticamente.

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.

Capítulo 6

Preguntas frecuentes de Junos Pulse

Este capítulo ofrece respuestas a las preguntas más frecuentes.

Preguntas frecuentes de Junos Pulse

No quiero que el usuario del dispositivo vea la aplicación Junos Pulse en el dispositivo. ¿Puedo ocultarla?

Sabemos que en algunos dispositivos pueden ocultarse los iconos, pero la aplicación Junos Pulse no puede ocultarse. Además del control y la supervisión, Junos Pulse ofrece funciones de seguridad que requieren el acceso del usuario final para poder configurarse.

¿Qué ocurre si el usuario del dispositivo modifica los ajustes de Junos Pulse en el dispositivo?

En función de la modificación realizada, ésta puede no aparecer en el panel de Mobile Security. Por ejemplo, si el usuario del dispositivo desinstala Junos Pulse del dispositivo, este evento no se mostrará en el panel de Mobile Security. Simplemente se observará una ausencia de eventos.

¿Por qué son imprecisas las coordenadas de mi GPS?

Esta imprecisión puede deberse a varios motivos. En primer lugar, confirme que tiene un dispositivo con GPS habilitado y que el GPS entra dentro del plan de datos de su portadora. Si la funcionalidad de GPS no forma parte del servicio de red, la función de GPS no funcionará. Asimismo, compruebe que la función de GPS del dispositivo para asegurarse de que no existen restricciones y que todas las funciones se han habilitado. Establezca su ubicación con el dispositivo ayudándose de Google Maps desde un lugar en el que reciba una buena señal de la portadora. El mejor lugar para probar esto es el exterior. La señal del GPS puede también llegar a través de satélite o de la red, con diversos grados de precisión.

¿Qué significan las coordenadas 0.0 del GPS?

Normalmente, 0.0 indica que la portadora debe activar el GPS del dispositivo o que esta función la ha bloqueado la portadora para que no la usen aplicaciones de terceros. (Tenga en cuenta que no podemos garantizar la funcionalidad del GPS en los dispositivos Verizon BlackBerry Curve ni Storm 1).

Copyright © 2011, Juniper Networks, Inc.

¿Cuánto tiempo tarda el panel de Mobile Security en actualizar las actividades del usuario del dispositivo?

Esto puede configurarse desde el panel. Consulte “Administración del teléfono” en la página26 para obtener más información y directrices. (Tenga en cuenta que si el usuario del dispositivo envía y recibe un gran volumen de mensajes de texto, no es aconsejable el envío de dichos mensajes al panel en tiempo real).

¿Puedo utilizar Junos Pulse para supervisar o bloquear URL?

No, Junos Pulse no ofrece esta funcionalidad en estos momentos.

¿Cuántos dispositivos puedo supervisar usando el panel de Mobile Security?

No existe límite en el número de dispositivos que puede supervisar en una cuenta. Para agregar un dispositivo nuevo a la cuenta, deberá primero descargar el software al dispositivo adicional. Una vez que el dispositivo se registre con el panel, podrá supervisarlo.

Quiero supervisar varios dispositivos, pero cada uno utiliza una portadora diferente.

La portadora es irrelevante. Con tal de que el dispositivo utilice un sistema operativo compatible, podrá utilizar Junos Pulse.

Copyright © 2011, Juniper Networks, Inc.

Índice

A

Acuerdo de licencia de usuario final
- Android 4
- BlackBerry 9
- iOS 11

Administración de cuentas 26
Administración del teléfono 26
Ajustes 26
ajustes de seguridad
- Android 48

Alertas 30
Android
- ajustes de seguridad 63
- antivirus 40
- código de licencia 39
- conectando de forma segura 36
- funciones de seguridad 33
- instalar 3
- registro automático 38
- registro manual 39
- supervisión y control 47

Antirrobo
- Windows Mobile 70

Antivirus
- actualizaciones de firmas 64
- ajustes para Windows Mobile 64

antivirus 40
- actualización de definiciones, Android 41
- ajustes para BlackBerry 52, 55
- análisis a demanda, BlackBerry 54
- análisis completo, BlackBerry 52
- análisis manual, BlackBerry 52
- análisis personalizado, BlackBerry 52
- analizar archivo o carpeta, Android 41
- archivos en cuarentena, BlackBerry 53
- registro de supervisión de archivos, BlackBerry 54
- ver aplicaciones sospechosas permitidas, Android 41
- ver resultados de análisis, Android 41

aplicaciones de malware
- Android 44

aplicaciones prohibidas
- Android 43

aplicaciones sospechosas
- Android 45
- permitidas, Android 46

aplicaciones sospechosas permitidas
- Android 41
- pantalla Android 46

B

BlackBerry
- actualizar ajustes 55
- antivirus 51
- frecuencia de actualización automática 55
- funciones de seguridad 51
- instalar 9
- respaldo & restaurar 54
- supervisión y control 54
- tipo de conexión 55

Bloquear al cambiar SIM 27
bloquear dispositivo 22, 23, 56
Bloqueo de código breve 65
borrar datos
- Android 50

botón de llamada de emergencia, Android 49
botón de llamada de emergencia, BlackBerry 55

C

cambio de nombre de usuario/contraseña 26
certificado APNS 23
código de licencia 6
- Android 39

comandos 22
comandos, dispositivos iOS 23
conectando
- agregar una conexión, Android 35
- Android 35, 36
- certificado, Android 35
- certificado, iOS 60
- clave, Android 35
- estado, iOS 60

Copyright © 2011, Juniper Networks, Inc.

icono de estado, Android 36
iOS 57, 60
nombre, iOS 60
pantalla de estado, VPN completa, Android 37
URL 60
URL, Android 35
Conexión
Windows Mobile 61
conexión segura 36
Cortafuegos
Windows Mobile 66

D

desbloquear dispositivo 22, 23, 56
desinstalar
Android 50
detección de malware
Android 42
dispositivos con WIFI solamente 5

E

estado
Android 34
eventos de antivirus 24

F

funciones
información general de control 1
información general de seguridad 2
funciones antirrobo 49, 55
activación y desactivación de alarma 50, 56
bloquear dispositivo, Android 49
bloquear y desbloquear, BlackBerry 55
botón de llamada de emergencia, Android 49
botón de llamada de emergencia, BlackBerry 55
cambio de SIM 50, 56
desbloquear dispositivo, Android 49
enviar respaldo 50, 56
GPS por robo 50, 56
limpiar dispositivo, Android 49
ubicación por GPS 50, 56
funciones de seguridad 56
Android 4, 33, 38
antivirus 10
BlackBerry 9, 10, 51
bloquear dispositivo 56
código de licencia 6
código de licencia, Android 39
desbloquear dispositivo 56
iOS 56
limpiar dispositivo 56
recuperar lista de aplicaciones 56
registrar, Android 4, 38
registrar, BlackBerry 9
registro automático de URL 4
registro automático de URL, Android 38
registro manual, Android 5, 39
respaldo y restaurar 10
supervisión y control 10

G

GPS
información de admisión para iOS 23
período de actualización 27
seguimiento de ubicación para iOS 15
gritar ubicar 23

H

Historial
comandos 30

I

icono de notificaciones
Android 42
instalación
Android 3
BlackBerry 9
información general 3
iOS 11
Windows Mobile 16
iOS
conectar de forma segura 57
funciones de seguridad 56
habilitar Junos Pulse 12
instalar perfil de seguridad 13
registro de URL automático 11
seguimiento de ubicación por GPS 15

L

Limpiar al cambiar SIM 27
limpiar dispositivo 23, 56

P

Palabras clave, mensajes abreviados 31
Panel de Mobile Security
administración de cuentas 26
administración del teléfono 26
alertas 30
información general 21
informes 29
pantalla de resultados de análisis
Android 41, 42
prohibida 43

Copyright © 2011, Juniper Networks, Inc.

R

recuperar lista de aplicaciones. 23, 56
Registrar límites de eventos. 27
Registrar límites de tamaño. 27
registro
  Android 3
  BlackBerry 9
  iOS. 11
  manual 10
  Windows Mobile 16
registro automático de URL. 4
  Android 38
registro de URL
  iOS. 11
registro manual
  Android 5, 39
Reportes. 29
respaldar datos
  Android 47
  BlackBerry 54
Respaldo & Restaurar
  Windows Mobile 69
respaldo & restaurar 22
restaurar datos 48
resultados de análisis
  aplicaciones prohibidas, Android 43
resultados del análisis
  malware, Android 44
  sospechosas, Android. 45
  virus, Android 47

S

Supervisar y controlar
  Windows Mobile. 69
supervisión de correo electrónico. 26
Supervisión de imágenes. 27
Supervisión de imágenes Web 27
supervisión de MMS. 27
supervisión de SMS 26
Supervisión de voz 27

U

ubicar dispositivo 22

V

ver más
  eventos. 24
virus
  Android. 47
  BlackBerry. 51

W

Windows Mobile
  antispam 64
  antivirus 63
  archivo .CAB. 17
  correo electrónico 61
  instalar 16
  intranet. 61
  respaldar datos. 69
  supervisión y control. 69

Copyright © 2011, Juniper Networks, Inc.

Copyright © 2011, Juniper Networks, Inc.